



TASK ORDER (TO)

47QFCA22F0025

Technical, Analytical, and Business Operations Services (TABO)

in support of:

Department of Defense Cyber Crime Center (DC3)



**Issued to:
Perspecta Enterprise Solutions LLC**

**Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405**

April 26, 2022

FEDSIM Project Number 47QFCA21Z1198

Task Order 47QFCA22F0025
Modification P00001

SECTION C – PERFORMANCE WORK STATEMENT

C.1 BACKGROUND AND AGENCY MISSION

The Department of Defense (DoD) Cyber Crime Center (DC3) was unofficially formed in 1998 as an entity under the Department of the Air Force (AF). The initial operational capability brought together the Defense Computer Forensics Laboratory (DCFL) and the Defense Computer Investigations Training Program (DCITP). DC3 is now designated as one of seven Federal Cybersecurity Centers by the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 and a DoD Center of Excellence by DoD Directive (DoDD) 5505.13E.

Since the foundation, DC3 has operated as a unit aligned under the Department of the AF Office of Special Investigations (OSI). DC3 is now designated in 2021 as a Field Operating Agency (FOA), aligned as a separate agency under the Inspector General, Office of the Secretary of the AF.

The DC3 is a DoD technical center for digital and multimedia (D/MM) forensics, cyber training, technical solutions Research and Development (R&D), cyber analytics, and vulnerability sharing supporting DoD and National requirements in: Law Enforcement and Counterintelligence (LE/CI), Document and Media Exploitation (DOMEX) and Counterterrorism (CT), and Cybersecurity (CS) and Critical Infrastructure Protection (CIP).

DC3's mission is to set the standards in D/MM forensics, develop and deliver specialized cyber investigative training, and serve as a focal point for information sharing on CS matters across the DoD. Also, DC3's mission is to deliver superior D/MM lab services, cyber technical training, technical solutions development, and cyber analytics for the following DoD mission areas: CS and CIP, LE/CI, document and media exploitation (DOMEX), CT, and safety inquiries.

Located in Linthicum, Maryland, DC3 components serve the DoD and other United States (U.S.) Federal agencies throughout the world. The DC3 organization consists of a mix of military, civilian, and contractor support personnel. The DC3 environment is dynamic and constantly evolving, with frequently changing priorities.

DC3 is operationally organized into six operational Directorates and two support Directorates, each with interrelated missions and support requirements that contribute to the overall mission.

Operational Directorates:

- a. Cyber Forensics Laboratory (DC3/CFL)
- b. Technical Solutions Development (DC3/TSD)
- c. Cyber Training Academy (DC3/CTA)
- d. DoD-Defense Industrial Base Collaborative Information Sharing Environment (DC3/DCISE)
- e. Operations Enablement Directorate (DC3/OED)
- f. Vulnerability Disclosure Program (DC3/VDP)

Support Directorates:

- a. Business and Technology Operations (DC3/BTO)
- b. Enterprise Management and Resourcing (DC3/ER)

Task Order 47QFCA22F0025
Modification P00001

PAGE C-1

SECTION C – PERFORMANCE WORK STATEMENT

C.2 SCOPE

The scope of the TO is to provide support services to seven of DC3's eight Directorates and the Judge Advocate (JA) office. The scope also includes providing support services to DoD, U.S. intelligence agencies, U.S. law enforcement agencies and the Department of Homeland Security in collaboration and pursuit of their shared Cyber Crime mission. These services include technical analysis, cyber forensics, technology solutions development, support for the Defense Industrial Base (DIB), Cyber Crime intelligence analysis, and cyber security support. Below is the mission for each DC3 Directorate under the scope of the TO:

- a. **CYBER FORENSICS LABORATORY (DC3/CFL):** Perform D/MM forensic examinations, device repair, data extraction, and expert testimony IAW International Organization for Standardization (ISO)17025 American National Standards Institute (ANSI) National Accreditation Board (ANAB) standards. Conduct intrusion, malware, and other CS analysis in support of the DC3 mission. Provide administrative and programmatic support as necessary.
- b. **TECHNICAL SOLUTIONS DEVELOPMENT (DC3/TSD):** Tailor software and system solutions engineered to the specific requirements of digital forensic examiners and cyber intrusion analysts. Validate commercial off-the-shelf (COTS), Government Off-the-Shelf (GOTS), and custom-developed software/hardware before it can be used in a forensic process. In addition, DC3/Technical Solutions Development (TSD) functions as the DoD repository for cyber Continuous Integration (CI) tools.
- c. **DoD-DEFENSE INDUSTRIAL BASE COLLABORATIVE INFORMATION SHARING ENVIRONMENT (DC3/DCISE):** Support DC3 with assisting DIB companies to safeguard DoD content and intellectual property residing on or transiting their unclassified networks. The contractor shall develop and share actionable threat products, and perform cyber threat analyses, diagnostics, and remediation consults for DIB Partners; support Cybersecurity-as-a-Service (CSaaS) pilot programs; develop, plan, and execute DIB company outreach and engagement events; and support and improve standard, repeatable process IAW the Capability Maturity Model for Integration (CMMI) for Services.
- d. **OPERATIONS ENABLEMENT (DC3/OED):** Amplify the effects of DoD-wide LE/CI investigations and operations, and by extension, the effects of the U.S. Intelligence Community (USIC) at large. Conduct sharply focused technical and cyber intelligence analysis leveraging multiple sources of data, unique analytic tools, applications, and capabilities to directly support stakeholder requirements and priorities. Support joint operations by managing the development, sustainment, and enhancement of operational support systems. Support DC3's role as a Federal Cyber Center including collaborative analytical and technical exchanges with Subject Matter Experts (SMEs) from LE/CI, Computer Network Defense (CND), USIC, and other CS agencies.
- e. **VULNERABILITY DISCLOSURE PROGRAM (DC3/VDP):** Support DC3's role in the Vulnerability Disclosure Program as approved by the Secretary of Defense, which authorizes private-sector CS researchers (i.e., white-hat Hackers) to scan publicly-accessible DoD information systems for vulnerabilities. DC3 is the sole focal point for receiving vulnerability reports and interacting with researchers. DC3 ensures that reports

SECTION C – PERFORMANCE WORK STATEMENT

are delivered to the system owner and remediation personnel as quickly as possible IAW the VDP Concept of Operations (CONOPS) and DoD Instruction (DoDI) 8531.01.

- f. **ENTERPRISE MANAGEMENT AND RESOURCING (DC3/ER):** ER supports DC3's mission to provide effective and efficient management of DoD/AF resources that are linked to strategic planning, budgeting, and performance reporting; and serves as the command's focal point for requirements management and associated processes.
- g. **BUSINESS AND TECHNOLOGY OPERATIONS (DC3/BTO):** BTO is the support element of DC3 and provides multiple functions critical in the achievement of DC3's mission: Human Resources (HR), Security Administration (SEC), Information Technology (IT), CS, Plans and Policy (XP), Information Management (Knowledge Management and Record Management), Enterprise Architecture (EA), IT Portfolio Management, Facilities (FAC), Public Affairs (PA), and Logistics (LG) that enable operations in a complex dynamic cyber environment. This requirement supports IT operations.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

DC3's IT services are maintained IAW all DoD and AF directives, guidelines, and requirements such as (but not limited to) DoDD 8570, AF Manual (AFMAN) 33-285 and AFMAN 33-282. DC3 operates and maintains one Non-classified Internet Protocol (IP) Routing Network (NIPRNET), one Secret Internet Protocol Routing Network (SIPRNET), one Joint Worldwide Intelligence Communications System (JWICS) and multiple stand-alone forensic/examination networks that provide processing and communications support. The DC3 Information Technology Division (ITD) is currently responsible for 12 separate networks and telecommunications systems of all classification levels serving more than 400 users throughout the DC3 organization. ITD critical networks and systems currently consist of the Unclassified DC3 Enterprise Network (DEN), Classified Secure DC3 Enterprise Network (SDEN), DC3's Open Network (DC3ON), DC3/CFL Networks (ExLAN, IA LAN), and phone systems.

C.4 OBJECTIVE

The objective of the TO is to continuously optimize performance within the DC3 lines of business, prepare for foreseeable developments or changes to the mission, improve quality of products and services, maintain an optimally skilled workforce, and develop innovative solutions.

C.5 TASKS

The following tasks are in support of this TO and are detailed below.

- a. Task 1 – Program Management Support
- b. Task 2 – Cyber Forensics Lab (DC3/CFL) Operations Support
- c. Task 3 – DC3/TSD Operational Support
- d. Task 4 – DC3/DCISE Support
- e. Task 5 – DC3/OED Operations Support
- f. Task 6 – DoD Vulnerability Disclosure Program (VDP) Operational Support

SECTION C – PERFORMANCE WORK STATEMENT

- g. Task 7 – Enterprise Management & Resourcing (ER) Support
- h. Task 8 – Business & Technology Operations (BTO) Support
- i. Task 9 – Judge Advocate (JA) Office Support
- j. Task 10 – Optional DC3 Surge Support
- k. Task 11 – Optional External Customer Support

C.5.1 TASK 1 – PROGRAM MANAGEMENT SUPPORT

The contractor shall provide program management services under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall facilitate Government and contractor communications, use industry-best standards and proven methodologies to track and document TO requirements and activities to allow for continuous monitoring and evaluation by the Government, and ensure all tasks are accomplished IAW the TO. The contractor shall notify the FEDSIM Contracting Officer's Representative (COR) and DC3 Technical Point of Contact (TPOC) via a Problem Notification Report (PNR) (**Section J, Attachment E**) of any technical, financial, personnel, or general managerial problems encountered throughout the TO PoP.

C.5.1.1 SUBTASK 1.1 – ACCOUNTING FOR SERVICE CONTRACT REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this TO (**Section F, Deliverable 01**). The contractor shall completely fill in all required data fields using the following web address: <https://www.sam.gov>.

Reporting inputs will be for the labor executed during the PoP during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year.

C.5.1.2 SUBTASK 1.2 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall coordinate a Project Kick-Off Meeting five days after award (**Section F, Deliverable 02**) in conjunction with the Government in a manner approved by the Government. The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include the contractor's Key Personnel, the DC3 TPOC, the FEDSIM COR, the FEDSIM CO, and other Government stakeholders.

At least three workdays prior to the Project Kick-Off Meeting, the contractor shall provide a Project Kick-Off Meeting Agenda (**Section F, Deliverable 03**) for review and approval by the FEDSIM COR and DC3 TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

- a. Points of Contact (POCs) for all parties.
- b. Program Management Plan (PMP) discussion including schedules and tasks.
- c. Draft financial reporting format for Weekly Activity Reports (WAR).

SECTION C – PERFORMANCE WORK STATEMENT

- d. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
- e. Project Staffing Plan and status.
- f. TO Portal strategy/solution.
- g. Security discussion and requirements (i.e., clearances, building access, badges, and Common Access Cards (CACs)).
- h. TO administration and invoicing considerations.
- i. Transition activities and status.
- j. Other TO requirements.

The deliverables that shall be provided to the Government at the Project Kick-Off Meeting are listed in **Section F**.

The Government will provide the contractor with the number of Government participants for the Project Kick-Off Meeting, and the contractor shall provide the electronic copy of the presentation to all participants.

The contractor shall draft and provide a Project Kick-Off Meeting Minutes Report (**Section F, Deliverable 04**) documenting the Project Kick-Off Meeting discussion and capturing any action items.

C.5.1.3 SUBTASK 1.3 – PROVIDE A PROGRAM MANAGEMENT PLAN (PMP)

The contractor shall provide a PMP (**Section F, Deliverable 05**) that is based on the contractor's solution. The contractor shall utilize the PMP as the foundation for information and resource management planning as well as to inform the Government how the contractor will manage the TO. The contractor shall use a Work Breakdown Structure (WBS), a component of the PMP, during the performance of the task. The PMP is an evolutionary document that the contractor shall update as project changes occur and annually at a minimum. The PMP shall be delivered in an editable, unlocked Microsoft (MS) Word document. The contractor shall provide Government access to the PMP via the TO portal. The contractor shall provide services IAW the latest Government-approved version of the PMP.

At a minimum, the PMP shall:

- a. Describe the proposed TO management approach and contractor organizational structure.
- b. Describe the contractor's approach to risk management including processes, procedures, and format.
- c. Describe the communications approach to include rules of engagement between the contractor and the Government and communication mechanisms (e.g., Technical Status Meeting, In-Progress Review (IPR), and Personnel Status (PERSTAT) Report).
- d. Describe the contractor's Quality Control (QC) methodology for accomplishing TO requirements and objectives. This includes how the contractor's processes and procedures will be tailored to and integrated with the Government to ensure high-quality performance.
- e. Contain Standard Operating Procedures (SOPs) for all tasks and requirements in Task 1 as necessary.

SECTION C – PERFORMANCE WORK STATEMENT

- f. Include a staffing matrix of all personnel assigned to the TO and include, at a minimum, their position, client(s) supported, and duty station/assigned place of performance.
- g. Include the contractor's general operating procedures for:
 - 1. Travel.
 - 2. Work hours.
 - 3. Leave.
 - 4. Staff training policies.
 - 5. Problem or issue resolution.

C.5.1.4 SUBTASK 1.4 – PROVIDE A MONTHLY STATUS REPORT (MSR)

The contractor shall provide an MSR (**Section F, Deliverable 06**) per the MSR template (**Section J, Attachment F**). The MSR shall summarize the technical and managerial work performed by the contractor during the previous month, and shall include the following:

- a. Activities during the reporting period, by task (include ongoing activities, new activities, and activities completed, and progress to date on all above-mentioned activities). Each section shall start with a brief description of the task.
- b. Monthly performance metrics by task.
- c. Site status including issues impacting sites, personnel, and performance.
- d. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- e. Risk reporting including the identified risks, impacts, and risk resolutions.
- f. Personnel gains, losses, and statuses.
- g. Government actions required.
- h. Schedule including tasks, milestones, and deliverables; planned and actual start and completion dates for each task.
- i. Summary of contractor travel.
- j. Financial status including:
 - 1. Cumulative actual TO burn and projected cost of each CLIN, WBS, and task area, for the current option year.
 - 2. Up to date spend plan including baseline, actuals, and forecast.
 - 3. Cumulative invoiced amounts for each CLIN and WBS.
 - 4. ODCs CLIN tracking report showing pending commercial purchases, approved commercial purchases, costs, locations, and due dates.
 - 5. Total incurred cost, broken down by labor and ODCs, for the contractor's services rendered for international partners. The total cost incurred shall be tracked by individual event and per international partner.
- k. Schedule execution and forecast reports defined during the Program Baseline Review (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- l. Financial management reports defined during the Program Baseline Review which shall include rate and usage variance.

SECTION C – PERFORMANCE WORK STATEMENT

- m. Any overtime worked and/or invoiced for the reporting period shall be highlighted and detailed.
- n. Quantifiable projected costs (projected to be incurred) for each CLIN and or Government-defined Work Breakdown Structure (WBS) elements from the end of the reporting period to the end of the Option Period with monthly revisions, as necessary. Additionally, the report shall specifically identify projected and remaining costs by WBS for all work funded externally via Military Interdepartmental Purchase Request (MIPR).
- o. Variance explanations shall be reviewed for the top five variances that trip the variance thresholds defined during the Program Baseline Review.
- p. Time-phased manpower report by labor category.
- q. Description of proposed baseline solutions versus actual solutions provided.
- r. Any recommendations for change, modifications, or improvements in tasks or process.
- s. Any changes to the PMP.
- t. Contractor work initiatives, efficiencies, good-news stories, significant events, accomplishments, new undertakings, design and process improvements undertaken during the reporting period, and follow-up reports on prior initiatives.

C.5.1.5 SUBTASK 1.5 – CONVENE TECHNICAL STATUS MEETINGS

The contractor Program Manager (PM) shall convene a monthly Technical Status Meeting (**Section F, Deliverable 07**) with the DC3 TPOC, FEDSIM COR, and other Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings (**Section F, Deliverable 08**), including attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR.

C.5.1.6 SUBTASK 1.6 – DEVELOP AND MAINTAIN AN INTEGRATED MASTER SCHEDULE (IMS)

The contractor shall develop a baseline and forecast resource loaded IMS utilizing MS Project (2013 or later) (**Section F, Deliverable 09**). The contractor shall provide a Draft IMS NLT 15 days after TOA and a Final IMS NLT 30 days of TOA. The contractor shall provide monthly IMS reports (**Section F, Deliverable 10**). The contractor shall propose or use the DC3-approved WBS, data dictionary, and charge code structure and encompass all elements of cost needed to execute the entirety of scope (both Level of Effort (LOE) and discrete work) outlined in this TO. The WBS shall delineate specific scope areas (e.g., internal versus external customer scope). Tasks shall be decomposed into granular manageable activities. The contractor shall ensure the IMS is in compliance with Data Item Description-Management (DI-MGMT)-81861 Format 6.

In addition, the contractor shall:

- a. Provide all resources (labor categories or by individual) needed to execute the scope within the IMS.
- b. Provide all labor resources (hours and average rates) in the IMS.
- c. Provide all ODC and material resources (in dollars) in the IMS.

SECTION C – PERFORMANCE WORK STATEMENT

- d. Provide a time phase of all resources within the IMS.
- e. Develop and maintain an IMS baseline management process (approved by DC3).
- f. Conduct a monthly IMS Baseline and Forecast (submit updated baseline and forecast data no later than ten workdays after the end of the contractor financial period close).
- g. Document baseline changes with appropriate approvals.

C.5.1.7 SUBTASK 1.7 – PROGRAM BASELINE REVIEW

The contractor shall conduct program baseline reviews of the scope, schedule, and costs represented in the approved IMS and present the information to DC3 Directors, DC3/ER, DC3 TPOC, FEDSIM COR, and other relevant Government stakeholders. The contractor shall conduct a program baseline review (**Section F, Deliverable 11**) to be approved by the Government. The contractor shall conduct each baseline review within 90 calendar days of exercising an Option Period.

The contractor shall incorporate the following in the program baseline review:

- a. IMS Baseline Schedule (includes the scope of the entire base or option period).
- b. Time-phased Cost Plan by WBS and CLIN.
- c. WBS.
- d. Data Dictionary.
- e. Charge Code Structure.
- f. Variance Reporting Thresholds.
- g. Project Management Plan (PMP) and discussion including schedule, risk, tasks, etc.
- h. Draft Financial Report Format.

C.5.1.8 SUBTASK 1.8 – PROVIDE A QUARTERLY IN-PROCESS REVIEW (IPR)

The contractor PM shall convene a quarterly IPR meeting with, at a minimum, the DC3 TPOC, FEDSIM COR, and other Government stakeholders (**Section F, Deliverable 12**). The purpose of this meeting is to ensure the Government has all the required information to make decisions, manage stakeholders, and coordinate activities. The contractor shall provide minutes of these meetings (**Section F, Deliverable 13**), including attendance, issues discussed, decisions made, and action items assigned to the contractor, the DC3 TPOC, and the FEDSIM COR.

C.5.1.9 SUBTASK 1.9 – PROVIDE PERSONNEL TRACKING AND REPORTING

The contractor shall track all personnel supporting the TO via the PERSTAT Report (**Section F, Deliverable 14**). The Government will specify the information to be included in the PERSTAT at the Project Kick-Off Meeting.

The contractor shall assist the DC3 TPOC in maintaining the Government's PERSTAT Report and other management tools for tracking the contractor's availability against specific operational requirements.

SECTION C – PERFORMANCE WORK STATEMENT

C.5.1.10 SUBTASK 1.10 – DC3 DIRECTORATE BUSINESS AND ADMINISTRATIVE SUPPORT

The contractor shall support clerical work critical to the achievement of DC3's mission such as processing customer requests/submissions and assist in project status tracking for DC3 Directorates. Activities include updating Directorate-specific databases such as project management software, case management systems, electronic records management systems, and knowledge management portals.

The contractor shall develop and maintain SOPs including annual review requirements for all business and administrative support activities (**Section F, Deliverable 15**). The contractor shall produce Weekly Activity Reports (WARs) (**Section F, Deliverable 16**) for appropriate Directorates.

The contractor shall provide business and administrative support services for DC3 and subordinate Directorates such as budget estimates assistance, records management, maintenance of computer data, long range planning assistance, drafting and editing official DC3 correspondence, such as reports, memos, press releases and internal communications, keeping inventories of equipment, routing incoming inquiries, coordinating and updating Master calendars and project schedules, coordinating DC3 visits, and coordinating travel and security documentation.

C.5.1.11 SUBTASK 1.11 – PROVIDE PROJECT MANAGEMENT

The contractor's TO governance structure shall be scalable to effectively support a multi-project environment under DC3 Surge Support (Task 10) and External Customer Support (Task 11), which is defined as supporting multiple Government entities with the need to separately track project management and contract elements such as requirements, deliverables, costs, and ceiling. The contractor shall use a WBS, a component of the PMP, during the performance of the task. During the life of the TO, the Government will require varying levels of support.

The Government will utilize the term Work Request (WR) to identify and track operational support needs. The Government expects that WRs will be issued at varying times within a PoP, and consisting of various appropriation types (e.g., one-year, two-year, no-year) depending on the bona fide need. These efforts can be severable or non-severable in nature, further impacting the level of tracking required to ensure that the Government maximizes the availability of funds. The Government will include the severability designation in the request for support.

C.5.1.12 SUBTASK 1.12 – PROVIDE A TO PORTAL

The contractor shall provide a TO portal that both Government-approved contractor personnel and Government personnel can access worldwide via a unique user Identification (ID) and password. The TO portal shall not be CAC-enabled and shall be a cloud-based solution available to users with a .mil or a .gov account. The contractor shall provide the DC3 TPOC and the FEDSIM COR with a recommended TO portal solution (**Section F, Deliverable 17**) at the Project Kick-Off Meeting. The contractor shall complete the portal no later than 30 calendar days following the Government's approval (**Section F, Deliverable 18**) and keep the data current.

SECTION C – PERFORMANCE WORK STATEMENT

The TO portal is to introduce efficiencies and ensure coordinated service delivery. At a minimum, the portal shall provide the following:

- a. Secure logical access controls with role-based views (e.g., FEDSIM COR and DC3 TPOC).
- b. A dashboard that displays the following:
 1. Client name
 2. Abbreviated work description
 3. Customer POC information
 4. Contractor POC information
 5. Allocated budget by CLIN and WBS
 6. Funded amount by CLIN and WBS
 7. Incurred cost amount by CLIN and WBS
 8. Invoiced amount by CLIN and WBS
 9. Burn rate by CLIN and WBS
- c. An automated workflow for Government review/approval of Requests to Initiate Purchase (RIPs) and Travel Authorization Requests (TARs), inclusive of the DC3 TPOC and FEDSIM COR. This workflow process shall also allow the FEDSIM COR, DC3 TPOC, and other Government personnel to provide digital concurrence and approval for RIPs and TARs.
- d. The ability to view financial information to allow the Government to track each effort's financial health. The Government will establish the level of granularity needed at the onset of an effort (e.g., funding document, line of accounting level).
- e. An organized document library to store TO deliverables (e.g., MSRs, PMP).

C.5.1.13 SUBTASK 1.13 – TRANSITION-IN

The contractor shall provide and present a Transition-In resource loaded MS Schedule that outlines all tasks and resources needed to successfully complete the transition-in (**Section F, Deliverable 19**) at the Project Kick-Off Meeting. Within three calendar days following the Project Kick-Off Meeting the contractor shall incorporate Government feedback and submit a baselined resource loaded MS Schedule that outlines all tasks and resources needed to successfully complete the transition-in. The contractor shall implement Transition-In Plan No Later Than (NLT) ten workdays after award. During transition-in, the contractor shall ensure minimal service disruption to vital Government business and no service degradation during and after transition. All transition activities shall be completed per the contractor's Transition-In Plan NLT 90 calendar days after Project Start (PS). As a part of transition-in, the contractor shall coordinate with the outgoing contractor and the Government to ensure all Government property is transferred to the incoming contractor.

C.5.1.14 SUBTASK 1.14 – TRANSITION-OUT

The contractor shall provide and present a Draft Transition-Out resource loaded MS Schedule that outlines all tasks and resources needed to successfully complete the transition-out (**Section F, Deliverable 20**) 120 -day completion of a seamless transition from the incumbent to an

SECTION C – PERFORMANCE WORK STATEMENT

incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a final Transition-Out resource loaded MS Schedule that outlines all tasks and resources needed to successfully complete the transition-out (**Section F, Deliverable 20**) NLT 90 calendar days prior to expiration of the TO Base Period. The final Transition-Out Plan (**Section F, Deliverable 20**) shall incorporate the Government's comments. The contractor shall review and update the Government-approved Transition-Out Plan on an annual basis, at a minimum, and the contractor shall review and update the Transition-Out Plan quarterly during the final Option Period (**Section F, Deliverable 20**). In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor or Government personnel to transfer knowledge regarding the following:

- a. Project/Program management processes.
- b. POCs.
- c. Location of technical and project/program management documentation.
- d. Status of ongoing technical initiatives.
- e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
- f. Transition of Key Personnel roles and responsibilities.
- g. Schedules and milestones.
- h. Actions required of the Government.
- i. RIP and TAR data for the life of the TO.
- j. Transition of all Government-Furnished Property (GFP) and supplies.
- k. Status of Communications Security (COMSEC).
- l. Data from the material management services including all equipment and supply consumption data for the life of the TO.
- m. Editable and final copy of all TO deliverables. The contractor shall establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

C.5.2 TASK 2 – CYBER FORENSICS LAB (DC3/CFL) OPERATIONS SUPPORT

DC3 operates an ANAB-accredited digital data/multimedia forensic laboratory called the Defense Cyber Forensics Laboratory (DC3/CFL). DC3/CFL conducts examinations on digital and multimedia items submitted to the lab for forensic analysis. DC3/CFL receives examination requests from across the reach and scope of the DoD. DC3/CFL conducts a wide variety of examinations to include, but not limited to, homicide, child sexual exploitation, sexual assault, identity theft, counterfeiting, misconduct, terrorism, intrusions, fraud, and misuse of Government property. DC3/CFL operates across various security classifications levels to include: CUI, TS, SCI, SAP, and SAR.

C.5.2.1 SUBTASK 2.1 – DC3/CFL INTAKE SUPPORT

The contractor shall support inbound customer service inquiries, including DC3/CFL forensic examination requests. The contractor shall assist with identifying potential case conflicts, evidential issues, and operational or policy impacts. The contractor shall recommend, update, and support the intake procedures for the Government's review and approval and identify forensic and scheduling requirements of customer requests.

Task Order 47QFCA22F0025

Modification P00001

PAGE C-11

SECTION C – PERFORMANCE WORK STATEMENT

C.5.2.2 SUBTASK 2.2 – DATA IMAGING AND EXTRACTION (I&E) SUPPORT

The contractor shall perform forensic imaging and extraction of digital information in support of forensic examinations to develop evidence and intelligence information. This work shall be completed IAW requirements set forth by Government and Federal law, the Uniform Code of Military Justice, CFL Accreditation and SOPs, and the DC3 Personnel Handbook. The contractor shall ensure data imaging and extraction of media is completed within specified timelines. The size and complexity of each forensic image is considered when determining actual suspense.

The contractor shall prepare and perform forensic imaging and extraction on a variety of digital media including computers and laptops, mobile devices, Internet-of-Things (IOT) devices, optical and removable media, Digital Video Recorders (DVRs), cameras, gaming devices, and others yet to be determined. The contractor shall have the expertise to assess new and esoteric devices that may contain data and identify methods for data extraction and imaging.

The contractor shall be required to provide on-site imaging and extraction at specific evidence sites and alternate operating locations. The contractor shall extract and duplicate forensically sound images of the media utilizing DC3/CFL-approved imaging tools. Once the evidence or original media is extracted and duplicated, the contractor shall archive all image files to appropriate storage media.

The contractor shall record, document, and maintain written notes throughout the forensic imaging process and input data into appropriate information systems. All forensic processes conducted by the contractor shall be documented IAW DC3 policies and procedures. The contractor shall perform repair and recovery of data from damaged media on all cases assigned by the Government. The contractor shall employ specialized techniques for damaged media recovery, hard drive repair, and CD/DVD-ROM disk resurfacing; and be able to produce restored copies of the suspect media for examination.

The contractor shall participate, present, and provide input at briefings, meetings, conferences, panels, boards, seminars, working group sessions, technical exchanges, and public forums on cyber-crime and forensic-related D/MM imaging and extraction in support of DC3.

C.5.2.3 SUBTASK 2.3 – EXAMINATION SUPPORT

The contractor shall support the planning, organization, and execution of digital forensic examinations for a broad range of evidence items submitted to DC3. This work shall be completed IAW requirements set forth by the Government and Federal law, the Uniform Code of Military Justice (UCMJ), CFL Accreditation and SOPs, and the DC3 Personnel Handbook.

Forensic analysis shall include exams in support of civil, criminal, other casework and cover a broad range of expertise areas. The contractor shall have capabilities in advanced forensic analysis including cryptography, malware reverse engineering, specialized mobile forensics, data recovery from damaged media, password cracking, unknown file system analysis, and other complex forensic processes as the need arises. Cases shall be assigned by the Government.

The contractor shall conduct malware analysis, reverse engineering software development, and other forensic activities spanning the cyber-attack lifecycle, from the initial exploit and malware execution path to callback destinations and follow-on binary download attempts.

SECTION C – PERFORMANCE WORK STATEMENT

The forensic examinations performed by the contractor shall follow industry-standard Digital Forensic processes that protect the integrity of the evidence and may include verification and comparison of the forensic image files; examination for the presence of malicious logic such as viruses, Trojans, or worms; examination of media for deleted files and folders; documenting active and recovered deleted files; analysis for misnamed files; conducting word searches; and analysis for relevant hardware and software configuration information.

The contractor shall conduct examinations off-site, at an alternate or temporary duty location, or in conjunction with ongoing investigations that require triage and analysis performed outside of typical lab procedures. In these instances, the contractor shall conduct these non-standard activities with the permission of the Lab Director and IAW lab policy.

The contractor shall write concise, comprehensive, and accurate notes throughout the examination process. The contractor shall also develop a complete D/MM Forensic Analysis Report (**Section F, Deliverable 21**) upon completion of the examination.

The contractor shall perform technical peer reviews and feedback of other examiner cases. The technical peer review process shall include reviewing other examiners' reports for technical accuracy, readability, and administrative compliance.

The contractor may be required to present findings of their work in Military, Federal, State, or local courts as an expert witness, and oftentimes with little notice. The contractor shall travel to CONUS and OCONUS court proceedings to provide testimony. The assigned contractor personnel shall possess a valid U.S. passport.

The contractor shall perform D/MM forensics examinations in support of the National Media Exploitation Center (NMEC). This support includes processing critical national intelligence level cases that require expert analysis on AV equipment, cell phones and other mobile devices, and analyzing information to determine useful data and content across a number of NMEC databases. The contractor shall perform audio and video forensics on commercial video systems and digital recording devices to extract, digitize, and enhance audio and video data for case agent review.

C.5.2.4 SUBTASK 2.4 – EVIDENCE CUSTODIAL SUPPORT

The contractor shall assist the Government in ensuring an effective evidence program is maintained and provide support services for all evidence entering and exiting DC3/CFL at the direction of the Government.

All contractor personnel assigned to the Evidence Room shall be trained to handle evidence IAW DC3/CFL and DoD policies. Upon completion of the training program, personnel shall be required to pass a written test to work in the Evidence Room.

The contractor shall receive, review, and maintain the integrity and proper custody of the evidence. The contractor shall identify and report any discrepancies in receipt of the evidence to the evidence custodian. The contractor shall ensure forensic processes, handling, and hardware utilized are designed to safeguard all submitted evidence. The contractor shall receive, inspect, and administratively process all incoming evidence, packages, and freight deliveries into the laboratory. Some items received may be large and the contractor shall be capable of handling heavy objects up to 50 pounds.

SECTION C – PERFORMANCE WORK STATEMENT

The contractor shall establish chain-of-custody documents for all evidence to document the transfer of the evidence within DC3/CFL. The contractor shall identify, photograph, store, and ensure all evidence is properly marked, tracked, and processed. The contractor shall record received evidence in CFL's various information management programs as directed by policy. In addition, the contractor shall assist in resolving evidence control problems and perform routine evidence audits.

The contractor shall create, update, and maintain case folders containing all required forms and supporting documentation for the case. The contractor shall monitor and control the evidence in all aspects of laboratory operations and shall conduct reviews of all incoming and outgoing evidence chain-of-custody documents. The contractor shall be responsible for returning all evidence to the owning agency when the imaging and extraction process is complete. The contractor shall support the tracking and monitoring of all related shipping costs identifying all costs to the FEDSIM COR and DC3 TPOC for review.

The contractor will ensure that contractor personnel are available to staff evidence section requirements on a daily basis.

C.5.2.5 SUBTASK 2.5 – DC3/CFL QUALITY ASSURANCE

The contractor shall assist DC3/CFL in maintaining, updating, and managing the lab's Quality Assurance Program (QAP). The contractor shall support CFL's document control program and ensure appropriate controls, versioning, and updates are regularly maintained. This includes the issuance of lab orders, quality manual updates, and creating or updating other lab-related documents.

The contractor shall also be responsible for managing documents and controls related to examiner qualifications, education, and prior testimony as well as documents related to scientific procedures and methods. The contractor shall maintain the DC3/CFL QAP to include performance metrics to measure the lab's effectiveness, formal and informal reviews of analyses, and methods to ensure quality and customer satisfaction. This includes regular monthly metrics as well as ad-hoc reporting as required by the Government.

C.5.2.6 SUBTASK 2.6 – DC3/CFL TRAINING DEVELOPMENT AND MENTORING PROGRAM

To remain on the cutting edge of advances in D/MM forensic technology, DC3/CFL personnel require continual training. The contractor shall support DC3/CFL by monitoring, updating, and tracking all DC3/CFL personnel (contractor and Government) training through completion to maintain currency and adherence to the QAP. Currently, there is a 40-hour continuing education requirement for all examiners. Continuing education must be approved by Lab Management and requires a formal certificate of completion.

The contractor shall assist DC3 with establishing and maintaining requirements for a continuing education program for all D/MM examiners.

The contractor shall assist in developing and maintaining a remedial action plan to ensure all Forensic Examiners successfully complete proficiency tests as required by the QAP to perform forensic work in DC3/CFL.

SECTION C – PERFORMANCE WORK STATEMENT

The contractor shall provide training personnel in support of DC3 with a formal examiner mentoring program IAW DC3's SOPs. The contractor shall provide regular documentation on the effectiveness of the training and mentorship program and provide input on strategies for improvement.

C.5.3 TASK 3 – DC3/TSD OPERATIONAL SUPPORT

The contractor shall assist the DC3/TSD with its mission to provide legally and scientifically accepted standards, techniques, methodologies, research, tools, and technologies on digital forensics and cyber threat analysis to meet current and future threats.

The contractor shall assist DC3/TSD with pioneering digital forensic and cyber threat analysis tools, processes, and procedures to ensure DC3 remains on the leading edge of the discipline.

The contractor shall assist DC3/TSD in managing the planning, programming, and execution of program and infrastructure requirements linked to advancing digital forensic and cyber threat analysis research, development, test, and evaluation efforts.

C.5.3.1 SUBTASK 3.1 – DC3/TSD RESEARCH AND SYSTEMS DEVELOPMENT

The contractor shall assist with the planning, design, development, and deployment of digital forensics and cyber threat analytical capabilities. The TSD Solutions and Software to be developed by the contractor under this subtask consist of short to long term software development projects (**Section F, Deliverable 22**). The new development projects range from large, complex modernization efforts to a smaller file parsing effort.

[Proposal Purposes Only] Historically, new development projects of large scale have required five or more resources or full-time equivalents, medium scale projects up to four resources, and smaller scale projects up to two resources. On average per year, DC3/TSD does approximately four large scale projects (greater than 240 hours for development and IT support) and nine small scale projects (less than 240 hours for development and IT support). Each year, there are approximately ten Operations and Maintenance (O&M) projects that require approximately four releases each.

The contractor shall support the incoming project requirements at DC3/TSD which are generated from internal DC3 customers (Directorates) as well as external customer agencies (e.g., SOCOM, Military Department Counterintelligence Organizations (MDCOs), NMEC). Customer engineering requests are delivered to DC3/TSD through submissions to the current System of Record (DC3 Enterprise Support Center – TSD Support).

The contractor shall support the requirements for submitting new projects through the DC3's Baseline Change Control Process. The contractor shall assist DC3/TSD with creating, reviewing, prioritizing, and tracking requests.

The contractor shall review requests for existing solutions as well as commonalities with other solutions and document those identified commonalities.

The contractor shall ensure all established requirements requests are in line with agency regulations, Federal law, the UCMJ, DC3 SOPs and Quality Assurance guidelines, and the DC3 Personnel Handbook in developing computer software and performing forensic tests of computer forensic software. In the event that a request is outside the scope of or problematic to such

Task Order 47QFCA22F0025

Modification P00001

PAGE C-15

SECTION C – PERFORMANCE WORK STATEMENT

regulations, the contractor shall provide a written analysis for the Government's review and approval.

The Government's desire is to use COTS or already existing GOTS products (hardware/software) at DC3. During the Technical Assessment (TA) phase of the Baseline Change Control Process, the contractor shall complete an analysis of alternatives by identifying existing COTS and GOTS solutions.

The contractor shall be responsible for creating the system concept, capturing requirements, design, development, testing, deployment, and O&M.

The contractor shall, for all priority projects as defined by the Government, develop a project IAW the DC3/TSD System Development Lifecycle SOP and Baseline Change Control Process. All projects shall be tracked as TSD Project Tracker in the DC3 Integrated Master Schedule (**Section F, Deliverable 23**).

The contractor shall work with all system stakeholders during requirements gathering to ensure the requirements are accurate, documented, and approved before design. The contractor shall adhere to the requirements management plan. The design plan shall be approved by the Government before development and integration.

The contractor shall ensure systems development efforts adhere to the applicable design specifications.

The contractor shall adhere to the guidelines specified in the DC3/TSD System Development Lifecycle SOP, unless otherwise specified by the Government, including but not limited to secure coding practices following the RMF. The contractor shall recommend and propose changes to the Government for approval to facilitate DevSecOps processes. Where appropriate, the applications should utilize containerization and be hosted in the appropriate environments whether that be on premises systems, Kubernetes-based systems, or cloud infrastructures.

Prior to deployment, the contractor shall provide test and evaluation support on systems to be deployed through User Acceptance Testing (UAT). The contractor's UAT results shall include, but are not limited to, discrepancies, recommendations, and corrections. The contractor shall document all relevant information in the DC3/TSD System of Record for project management.

The contractor shall develop a deployment plan and prepare production environments (e.g., build or write scripts) in collaboration with ITD/CS/EA. The contractor shall ensure operational readiness with all appropriate stakeholders prior to deployment.

The contractor shall support O&M of deployed and operational systems. System O&M activities include, but are not limited to, bug fixes, system enhancements, preventative maintenance, CS required updates and technical refresh.

The contractor shall coordinate with all appropriate stakeholders when conducting O&M activities and track all requirements. All system enhancements require a formal project plan and coordination with EA.

The contractor shall provide technical editing support for documents such as, but not limited to, validations reports, requirement and design documents, and memorandums for the record (MFRs). The technical editor shall collaborate with developers, testers, and SMEs and ensure that each piece of content meets organizational objectives.

Task Order 47QFCA22F0025

Modification P00001

PAGE C-16

SECTION C – PERFORMANCE WORK STATEMENT

For specific project requirements, the contractor shall directly support operational needs in DC3/CFL, DC3/AG, DC3/VDP and DC3/DCISE by embedding developers to work alongside forensic examiners, intrusion analysts, and cyber threat analysts. The contractor shall track such operational support activities, including the need fulfilled, time spent, and operational impact. When such operational support generates a new tool, process, or procedure that can be reused by others, the contractor shall assist with transitioning new capabilities to be a part of DC3's routine/automated processes.

The contractor shall provide an electronic WAR to include updates of status and progress of current and upcoming projects. The contractor shall track projects' status and identify time accrued on particular requests. The contractor shall prepare monthly briefings on the progress, outcome, or evaluation of requirements.

The contractor shall gather, analyze, and prioritize existing research and informal studies to identify and collect publicly available information/tools to support and enhance DC3/TSD research and development activities leading to technical solutions. Based on findings, the contractor shall provide written analysis and recommendation of further DC3/TSD research and development ideas/strategies as needed for the Government's consideration.

The contractor shall document research, analysis, studies, and recommendations in written technical reports, information, point, practice advisories, white papers, and decision papers.

The contractor shall participate, present, and provide input at briefings, meetings, conferences, panels, online forums, boards, seminars, working group sessions, technical exchanges, and demonstrations and public forums for/on cyber-crime and forensic-related IT media research and development in support of DC3.

C.5.3.2 SUBTASK 3.2 – TESTING AND EVALUATION

The contractor shall assist DC3/TSD with the planning, establishment, and operations for tests, validations, and evaluations of computer, computer forensic processes, hardware and/or software in compliance with the DC3 Test and Evaluation Instructions. Validations are completed for DC3/CFL IAW the ANAB. Testing and Evaluation Projects include, but are not limited to, creating test data sets, developing a test plan, carrying out the tests in a scientific manner, and generating reports outlining the test findings along with any anomalies and/or observations which could prove useful to digital forensic examiners when employing the given tool or procedure (**Section F, Deliverable 24**).

The contractor shall, upon Government request, prepare Project Status Review presentations (**Section F, Deliverable 25**), which serve to document the steps undertaken by the contractor to validate that a given digital forensic tool, process, or procedure is forensically sound.

The contractor shall assist in automating the testing process. The contractor shall gather, analyze, and prioritize existing data to identify and document possible testing scenarios and additional required hardware, software, or internal/external support required to complete the test IAW the scheduled timeframe (i.e., validation of commercial tools, testing of in-house developed software, enterprise project).

SECTION C – PERFORMANCE WORK STATEMENT

The contractor shall communicate, meet, and interface as a part of a team with other members assigned to a project including but not limited to developers, project managers, other testers, customers, IT support, and CS.

C.5.4 TASK 4 – DC3/DCISE SUPPORT

DC3/DCISE's mission enables protection of DoD information on DIB unclassified networks by fostering a collaborative information sharing environment and delivering DIB-focused CS services & resources. DC3/DCISE also serves as the focal point for all DIB cyber incident reporting affecting unclassified networks and providing awareness across the U.S Government of CS threats and trends that impact the DIB. DC3/DCISE supplies all source-derived relevant analysis including methods, indicators, and targeting objectives, while coordinating the collection and forensic analysis of submitted media/malware. The contractor shall produce WARs for Directorate under this subtask. (**Section F, Deliverable 16**).

[Proposal Purposes Only] The DIB CS Program supported approximately 782 DIB member companies at close of FY 2020. DIB CS Program participation is expected to grow by no more than 9% over the life of the TO. The contractor shall be required to adjust staff resources and operations accordingly to support the program participation growth.

C.5.4.1 SUBTASK 4.1 – DEFENSE INDUSTRIAL BASE CYBERSECURITY (DIB CS) PROGRAM OFFICE AND POLICY SUPPORT

The contractor shall serve as a liaison for DC3 and provide subject matter expertise to DoD's DIB CS Program Office within the office of the DoD CIO to include communication on DC3 equities on DoD and national policy, to prepare DoD cyber policy recommendations for agency consideration, represent DC3 at DoD and interagency forums, and assist the DIB CS Program Office on a day-to-day basis.

The contractor shall provide a range of subject matter expertise on DoD policy formulation, foreign cyber threats, DoD CI, the USIC, and DoD sensitive activities. The contractor shall interpret draft policy issuances and provide DC3 guidance on how they may impact the DC3 mission to support cyber threat information sharing, as well as its other mission areas in support of LE and CI investigative support activities (e.g., digital forensics and multi-media analysis for the Defense LE/CI Components, DoD cyber technical training, research, development, test, and evaluation, and cyber analytics).

The contractor shall perform outreach and represent DC3 and the DIB CS Program Office at specified Government and industry sponsored events, meetings, and conferences. The contractor shall attend, in person or virtually, DC3/DCISE Operations Meetings as required.

C.5.4.2 SUBTASK 4.2 – DC3/DCISE MISSION SUPPORT

The DC3/DCISE Mission Support Division is comprised of two branches: Customer Engagement (CE) and Organizational Readiness (OR). CE is the operational entry point for DIB Partners and USG Stakeholders. This branch is primarily responsible for all external customer support, including DIB Onboarding, Defense Industrial Base Network (DIBNet) Management and outreach services to promote DIB participation, communication and collaboration in the DIB CS Program, and DIB Partner Technical Exchanges. The OR branch is primarily responsible for

SECTION C – PERFORMANCE WORK STATEMENT

the internal DC3/DCISE training program, In/Out Processing of DC3/DCISE employees, Quality Control, Quality Assurance and managing CMMI for Services Level 3 efforts, managing the Metrics Database, Project Management, Requirements Management, and DC3/DCISE Knowledge Management.

The contractor shall develop, manage, and coordinate DIB partner outreach projects and collaborative initiatives. Projects and initiatives include, but are not limited to, outreach and communications events, campaigns, strategies, slick sheets, and other informational materials to promote the DIB CS Program and DCISE capabilities.

The contractor shall organize all logistics, facilities, and marketing aspects of DIB partner events (e.g., Technical Exchanges, Regional Partner Exchanges, Virtual Partner Exchanges).

The contractor shall serve as the primary POC for DIB partner outreach as well as requests for assistance and Frequently Asked Questions (FAQs) from Government and industry stakeholders.

Contractor support may require the use of diverse, multi-media equipment, including AV platforms, teleprompter, video documentation, lighting, sound reinforcement, interactive content, Video Teleconferencing (VTC) services, and online collaboration platforms. The contractor shall ensure that collaboration platforms are used IAW their security capabilities. In particular, the contractor shall ensure that no CUI/For Official Use Only data is stored or displayed on a system that is not properly accredited (currently the DoD requires the use of systems certified at Impact Level 4 or above).

The contractor shall develop and maintain SOPs for all CE activities (**Section F, Deliverable 26**).

The contractor shall manage DIB Partner records, engagements, and other appropriate data in the DC3/DCISE Customer Relationship Management (CRM) solution (currently Salesforce). The contractor shall develop ways to capture and automate DC3/DCISE process in the CRM.

C.5.4.3 SUBTASK 4.3 – DC3/DCISE ORGANIZATIONAL QUALITY ASSURANCE AND TRAINING

The contractor shall document organizational processes and procedures performed in DC3/DCISE and maintain information on a Government-accessible channel. The contractor shall ensure DC3/DCISE processes and procedures are documented and aligned with the Capability Maturity Model Integration for Services (CMMI-SVC) framework. The contractor shall lead CMMI-SVC (ML-3) re-appraisal efforts, including internal organizational coordination and collaboration, planning sessions, pre-audits, and third-party evaluation coordination. The contractor shall ensure these efforts are documented and maintained in MS Project.

The contractor shall provide subject matter expertise in requirements management to include documentation and maintenance of traceability matrices. The contractor shall provide subject matter expertise in project management and document DC3/DCISE efforts and progress towards the goals in the DC3/DCISE Long Range Strategic Plan.

The contractor shall provide compliance status updates to DC3/DCISE Leadership and the FEDSIM COR that offer recommendations to ensure successful re-appraisal. The contractor shall support DC3/DCISE by monitoring, updating, and tracking all DC3/DCISE personnel training through completion to maintain currency and adherence to CMMI requirements. The contractor

Task Order 47QFCA22F0025

Modification P00001

PAGE C-19

SECTION C – PERFORMANCE WORK STATEMENT

shall implement and manage formal training on DC3/DCISE processes and procedures, including technical job-related functions.

C.5.4.4 SUBTASK 4.4 – DIB PORTAL AND KNOWLEDGE MANAGEMENT SUPPORT

The contractor shall provide support for the classified and unclassified DIBNet portals and knowledge management in support of program operations.

The contractor shall provide DIBNet portal management (classified and unclassified) including, but not limited to, user account administration (add/delete/reset), coordination with ITD for DIBLan accounts, Public Key Infrastructure (PKI) Certification processing and tracking, troubleshooting user issues, on-boarding for new users, training, and other customer support requests.

The contractor shall notify DC3/DCISE of outages or other issues impacting the access and performance to DIBNet IAW DCISE standard processes for service issue management. The contractor shall develop metrics and track performance of DIBNet and recommend improvements to the overall DIBNet performance and processes.

The contractor shall develop and implement creative and effective ways to strategically capture and share technical knowledge, recommend processes and procedures, and improve the effectiveness of DC3/DCISE products and services.

The contractor shall monitor and maintain program content, including the development of ad-hoc reports, queries, and analyses. The contractor shall support customer requests (i.e., Requests for Information (RFIs)) and collection management from internal and external mission partners.

The contractor shall identify process improvement opportunities and develop a performance measurement framework for DCISE. The contractor shall maintain QC of all DCISE products. The contractor shall develop and maintain SOPs in support of the above.

C.5.4.5 SUBTASK 4.5 – DC3/DCISE CYBER THREAT ANALYSIS SUPPORT

The contractor shall perform cyber threat analysis for the DIB, on behalf of DC3/DCISE. The contractor shall support the DC3/DCISE mission while assigned to the Analytics Division. Subordinate to the Analytics Division are two branches: the Applied Research Branch and the Tactical Operations Branch.

The contractor shall provide support to analyze and triage partner reporting and ensure that threat, vulnerability, and mitigation information is disseminated in a timely and effective manner. This includes identifying indicators of compromise (IOCs), network threats, vulnerabilities, and exploits, and communicating with DIB Partner representatives.

The contractor shall conduct a variety of cyber intelligence gathering, including (OSINT) and closed source intelligence gathering, source verification, data fusion, and link analysis.

The contractor shall also conduct malware analysis on specific cases. The contractor shall develop analytical report products derived from analysis to assist partners with implementing defensive measures. The contractor shall be a proficient report writer, capable of expressing the results of research and analysis in published, serialized analytic reports.

SECTION C – PERFORMANCE WORK STATEMENT

The contractor shall:

- a. Perform acceptance of the initial reporting of cyber security events from DIB partners IAW the defined timeline and DC3/DCISE SOPs.
- b. Produce initial reports on severity of reported cyber security events IAW the defined timeline and DC3/DCISE SOPs.
- c. Perform data mining in support of customer requirements, to include basic tool development, database development, and other tasks as defined by best practice software development lifecycle management.
- d. Plan, coordinate, and execute off-site, bi-annual technical exchanges with external entities. At the Government's direction, these may be virtual due to pandemic restrictions.
- e. Coordinate and execute off-site Regional Partner Exchanges (RPEX) and Virtual Partner Exchanges (VIPEX) in coordination with MS/CE.
- f. Coordinate receipt of copies of malware (receiving copies of the actual offending software code and medium by which it was transmitted, which created the computer security event or incident), logs, and affected media.
- g. Develop and deliver Customer Response Forms (CRF) after receipt of Incident Collection Format (ICF) and/or Mandatory Incident Report (MIR).
- h. Develop and deliver Threat Activity Reports (TAR) after ICF receipt.
- i. Develop and deliver Cyber Targeting Analysis Reports (CTAR).
- j. Develop and deliver the daily Threat Information Product (TIP) Report notifying DIB Partners of possible threats to their network infrastructure, based on indicators derived solely from reports of intrusion activity in U.S. Government stakeholder networks.
- k. Develop and deliver CRF Supplements (amplifying information) to DIB Partners.
- l. Develop and deliver DCISE Alerts & Warnings within four hours for alerts or 24 business hours for warnings, respectively, of a reported incident or security event to help DIB Partners identify potential compromised systems within their networks.
- m. Develop and deliver Damage Assessment Management Office (DAMO) Nomination reports as necessary/applicable for further evaluation.
- n. Support development and delivery of annual updates to the DC3/DCISE Long Range Strategic Plan.
- o. Provide regular updates regarding threats and trends via report tracker and meetings.
- p. Develop Cyber Targeting Bulletins (CTB) reflecting U.S. Government current cyber intelligence/threat reporting.
- q. Submit requests, with DC3 approval, to reporting agencies for classification downgrades to ensure widest dissemination of information to the DIB; U or U//FOUO (or CUI, pending guidance from DoD CIO) is the goal.
- r. Develop ICF Trend Report, capturing metrics and trends of DIB threat reporting.
- s. Deliver Victim Notification (VN) to DIB Partner representatives.
- t. Deliver TIPPERS (i.e., products to DIB Partner representatives).
- u. Develop and deliver Weekly Indicator Roundups (WIR).
- v. Develop and deliver Cyber Incident Notifications (CIN).

SECTION C – PERFORMANCE WORK STATEMENT

- w. Possess understanding of U.S. Intelligence Community reporting and reporting repositories.
- x. Possess knowledge and understanding of classification markings and ability to handle and safeguard classified information.

[Proposal Purposes Only] DC3/DCISE currently supports 782 members in the DIB partnership. In FY 2019, the activity from the DIB partner community included 399 voluntary and 156 mandatory submission requirements. The DC3/DCISE Analytics Division produced 382 CRFs, 15 Supplements, 4 CTARs, 49 DCISE Alerts/Warnings, 13 TARs, and 259 TIPs, 30 CTBs, 5 VNs, 21 TIPPERS, 48 WIRs, 7 CINs, and 12 ICF Trend Reports.

The contractor shall provide QC support in the process of evaluating techniques, methods, and activities to consistently maintain product report quality standards. The QC support implements and manages the QC process used by DC3/DCISE prior to and after releasing all deliverables to internal and external stakeholders.

The contractor shall provide the Government leads with final products for peer review before delivery. The goal of QC is to provide the best quality product with minimal disruption to the workflow. QC reviews other DC3/DCISE publications and correspondence as well, including SOPs, training presentations, letters, briefing slides, conference brochures and papers, other communications.

The contractor shall identify technologies to increase the efficiency and effectiveness of analysis services, test technologies and create system/software development requirements for the DC3/TSD.

The contractor shall maintain DC3/DCISE related information on websites and via internal knowledge management resources across multiple classified environments and make recommendations to improve the overall operational effectiveness of these systems.

C.5.4.6 SUBTASK 4.6 – DC3/DCISE EXPANDED OFFERINGS AND PROJECTS SUPPORT

The contractor shall support the DCISE External Operations (XOP) Division CSaaS offerings, including support for new and emerging capabilities and services, such as PowerDNS (pDNS), DCISE3, and Malware Information Sharing Platform (MISP).

The contractor shall support the discovery of new pilot opportunities by identifying products and services outside of DCISE's current product/service portfolio.

The contractor shall provide support in the planning and execution of pilots. This activity includes, but is not limited to, developing the Pilot Initiation Statement, Analysis of Alternatives, identifying and onboarding of the Partners to participate in the pilot, and running the pilot for the duration of the agreement with the entity providing the pilot service.

The contractor shall develop after action reports upon the completion of a pilot. The contractor shall develop methods to analyze the data acquired from the pilots. This activity includes, but is not limited to, developing both manual and automated processes to ingest data from the pilot into existing and future repositories at DC3/DCISE, developing both manual and automated processes to analyze the data, and incorporating the resulting analysis into AD activities.

SECTION C – PERFORMANCE WORK STATEMENT

The contractor shall support the planning and execution of Cyber Resilience Analyses (CRA). This activity includes, but is not limited to, identifying partners for CRAs, performing the initial calls with the Partner, and finalizing the report to include debriefing the partner.

The contractor shall support the development and maintenance of an interconnection technology, hosted at DC3, to share IOCs in near real time with the Partnership. This activity includes, but is not limited to, discovery of the best solution available and working with applicable organizations at DC3 (e.g., ITD/TSD/CS) to instantiate that solution. The contractor may have to work with already existing capabilities and the entities that maintain them.

C.5.5 TASK 5 – DC3/OED OPERATIONS SUPPORT

The OED is composed of the Analytical Group (AG) and Capability Integration Group (CIG), both of which have unique operations support requirements.

OED/AG's mission is to provide highly focused technical and language enabled all-source analysis of cyber threats to the DoD in support of LE/CI partners and the USIC. The AG is composed of five regionally aligned branches and one production branch. Each branch is directed by a designated Government civilian. The contractor shall provide operations, analytic, and technical support for the OED/AG mission. The contractor shall provide a project management solution, inclusive of collecting and analyzing program and ad-hoc project metrics, resource management, quality assurance, and developing and implementing program improvements. The contractor shall support the development and execution of the AG analyst training program. The contractor shall identify technologies to increase the efficiency and effectiveness of analysis services, test technologies, and create system/software development requirements.

OED/CIG's mission is to provide support to the DoD counterintelligence community through the management of the evolution and development of the CADO-IS environment and an Automated Data Obfuscation capability. The contractor shall assist the DC3 with its mission to manage the CADO-IS program to enhance & integrate numerous cyber-based interagency and DoD counterintelligence capabilities to improve:

- a. Acquisitions & technology protection.
- b. DoD Information Network (DoDIN) & DIB network defense.
- c. DoD Cyber operations.
- d. Intelligence & counterintelligence operations.

For Automated Data Obfuscation the contractor shall assist the DC3 with its mission to provide Automated Data Obfuscation support to intelligence, counterintelligence, cyberspace operations, and program protection missions.

C.5.5.1 SUBTASK 5.1 – OED/AG MEDIA SUBMISSION AND PRODUCTION SUPPORT

The contractor shall coordinate all processing of media and malware cases submitted by OED/AG partner agencies for analysis. The contractor shall manage the workflow of all submissions to OED/AG for analysis and generate workflow statistics. The contractor shall provide a weekly update brief to AG leadership on the workflow.

SECTION C – PERFORMANCE WORK STATEMENT

The contractor shall provide technical editing support for all published products. The products shall maintain accuracy and standardization of format and style to AF, LE/IC, and USIC requirements. The contractor shall collaborate with writers and SMEs and ensure that each piece of content meets organizational objectives. The contractor shall support dissemination of all published products. The contractor shall appropriately store and update products as necessary with guidance from AG leadership.

The contractor shall provide processes and capabilities to manage RFI processing and track all incoming RFIs and RFI responses.

The contractor shall develop and deliver a WAR, which provides updates on the entire staff's activities during the preceding week and illustrates the current product production levels. In addition, the contractor shall provide monthly, quarterly, and annual production metrics and respond to ad-hoc production metrics requests from OED/AG leadership.

C.5.5.2 SUBTASK 5.2 – OED/AG ALL SOURCE CYBER ANALYSIS SUPPORT

The contractor shall conduct all-source cyber analytical/language fusion analysis in support of cyber investigations/operations and USIC requirements. The contractor shall support analysis and cuing for CI operations in cyberspace against Advanced Persistent Threats (APTs). The contractor shall provide a complete picture of the Tactics, Techniques, and Procedures (TTPs) used by malicious actors through fusion analysis of various data sources, including but not limited to, LE/CI community-furnished case data, technical collection, USIC reporting, open-source data, and DC3 data sources. Though “actionable intelligence” will be identified primarily for LE/CI organizations, the information may also be tailored to multiple consumers, to include computer network defenders; Signals Intelligence (SIGINT) and Human Intelligence (HUMINT) operators; intelligence analysts; and policy/decision makers. The contractor shall provide the following products and services:

- a. Develop and deliver Profile Reports (PRF) on individuals, organizations, and relationships associated with APT activity for investigative lead purposes.
- b. Develop and deliver Operational Lead Reports that augment technical intrusion data with cyber intelligence analysis. These reports are used as leads for investigative and operational purposes.
- c. Develop and deliver Persona Operational Lead Reports (POLR) to provide actionable leads on malicious cyber actors and their associates. These reports are used as leads for investigative and operational purposes.
- d. Develop and deliver all-source Cyber Intelligence Report (CIR) products on strategic and tactical aspects of APT activity, including but not limited to, targeting, TTPs, infrastructure, personas, organizational characteristics, and trends across multiple dimensions of APT activity.
- e. Develop and deliver Intelligence Information Reports (IIRs) for dissemination within the USIC IAW production timelines identified by OED/AG leadership.
- f. Develop and deliver Tailored Operating Picture (TOP) products that track APT activities over time as needed/requested by OED/AG leadership.

SECTION C – PERFORMANCE WORK STATEMENT

The contractor shall maintain a strict quality assurance process that inspects all products for analytic and technical accuracy. The contractor shall provide the designated Government analytic lead with final products for peer review before delivery.

C.5.5.3 SUBTASK 5.3 – OED/AG KNOWLEDGE MANAGEMENT SUPPORT

The contractor shall maintain OED/AG-related information on websites and internal knowledge management sources across multiple classified environments and make recommendations to improve the overall operational effectiveness of these systems.

The contractor shall develop and maintain SOPs for all OED/AG activities, including but not limited to, analytic/operational processes for each branch and broader Directorate processes related to analysis/production, operations support, external engagement, media analysis coordination, RFI processing, metrics tracking and reporting, and knowledge management processes (**Section F, Deliverable 27**).

C.5.5.4 SUBTASK 5.4 – OED/AG EXTERNAL ENGAGEMENT SUPPORT

The contractor shall lead collaborative analytical and technical exchanges with SMEs from LE/CI, CND, USIC, and IA agencies. Long distance travel (both CONUS and OCONUS) is anticipated to be required in support of these efforts. The objective of these exchanges is to build a threat picture to enable proactive cyber operations and anticipatory analysis focused on nation-state threat actors. In support of these efforts, the contractor shall:

- a. Develop analyst engagement opportunities, manage liaison functions, and deliver after action reports for each meeting.
- b. Provide embedded liaison support in key partner agencies identified by OED/AG leadership.
- c. Develop and deliver a Quarterly Meeting (**Section F, Deliverable 28**) on a quarterly basis featuring updates on APT activities and topics of interest by region to interagency analyst working groups.
- d. Create mission engagement materials as necessary.

C.5.5.5 SUBTASK 5.5 – REQUIREMENTS & CAPABILITIES ASSESSMENTS

The contractor shall establish and maintain regular, recurring communications with DoD and interagency consumers of information produced by counterintelligence cyber collections, investigations, and operations. The contractor shall identify and assess interagency and DoD cyber counterintelligence capabilities relative to identified stakeholder mission needs and provide recommendations to resolve capability gaps.

C.5.5.6 SUBTASK 5.6 – FACILITATE CADO-IS SUBPANEL OF DEFENSE CYBER OPERATIONS PANEL (DCOP)

The contractor shall provide meeting facilitation services for regular, recurring meetings of the DCOP CADO-IS Sub-Panel. This forum shall function as the primary mechanism to identify requirements and assess capabilities for prioritization by the DCOP members. This Sub-Panel is also responsible for coordinating and overseeing the design of technical solutions by DCOP member organizations and others to meet prioritized requirements.

SECTION C – PERFORMANCE WORK STATEMENT

C.5.5.7 SUBTASK 5.7 – CADO-IS ENTERPRISE ARCHITECTURE (EA) AND CONFIGURATION/INTEGRATION MANAGEMENT (CM)

The contractor shall establish and maintain the enterprise architecture based on direction from the Government PM and regular, recurring coordination with DCOP member organizations and other DoD and interagency stakeholders. The CADO-IS enterprise architecture shall be detailed in appropriate documentation and artifacts to reflect current state, proposed future state, and on-going development efforts. The contractor shall establish CM processes to enable the successful integration of systems and capabilities developed and managed by the DCOP member organizations and other stakeholders. This includes the development of a CADO-IS CMP (Section F, Deliverable 29) that identifies and establishes baselines for all CADO-IS configuration items across all participating organizations and tracks proposed changes to these configuration baselines to ensure effective and efficient operations.

C.5.5.8 SUBTASK 5.8 – MISSION PARTNER OUTREACH

The contractor shall establish and maintain regular recurring communications with DC3 mission partners to educate them on Automated Data Obfuscation capabilities supporting intelligence, counterintelligence, cyberspace operations, and program protection missions. The contractor shall maintain a record of these engagements.

C.5.5.9 SUBTASK 5.9 – MISSION PARTNER TRAINING

The contractor shall assist mission partners requesting Automated Data Obfuscation capabilities to access and receive online training on the system. The contractor shall maintain a record of mission partner personnel accessing and completing Automated Data Obfuscation training.

C.5.5.10 SUBTASK 5.10 – MISSION PARTNER MANAGEMENT

The contractor shall provide assistance services for mission partners in completing required user agreements and routing the agreements for required signatures. The contractor shall provide support to mission partners with using Automated Data Obfuscation capabilities to generate obfuscated files for placement on targeted networks/systems. The contractor shall maintain regular, recurring contact with mission partners to monitor for collateral exposure of obfuscated files. The contractor shall provide Tier 1 support to Automated Data Obfuscation users and shall coordinate required Tier 2 support with DC3 ITD. The contractor shall document new system and/or process requirements identified by users for coordination with Automated Data Obfuscation capability developers. The contractor shall ensure the proper disposition of obfuscated files upon completion of mission partner operations.

C.5.5.11 SUBTASK 5.11 – COLLATERAL EXPOSURE MITIGATION

Upon notification of exfil or unauthorized access to obfuscated files on targeted networks/systems, the contractor shall provide recommendations for establishing new intelligence collections and network defense requirements for the Government's review and approval. The contractor shall take appropriate mitigation actions if intelligence or network defense reporting indicates obfuscated files have been observed in blue or gray space.

**C.5.6 TASK 6 – DOD VULNERABILITY DISCLOSURE PROGRAM (VDP)
OPERATIONAL SUPPORT**

The contractor shall assist the DC3 with its mission to improve defense of the DoDIN by managing capabilities to receive, validate, triage, and coordinate CS vulnerabilities reported by private-sector white hat security researchers.

The contractor shall assist DC3 to track and analyze reported vulnerabilities and mitigation actions by system owners to identify gaps in customer cyber defenses and areas requiring increased attention, innovative assessments, and areas for improvement.

**C.5.6.1 SUBTASK 6.1 – RECEIVE, VALIDATE, TRIAGE, AND COORDINATE VDP
REPORTS**

The contractor shall receive, validate, triage, and coordinate vulnerability reports from private-sector white hat security researchers submitted under the VDP. The contractor shall review all VDP reports to determine if they are within the scope of the VDP policy and compare new VDP reports with previously submitted VDP reports to identify duplicates. The contractor shall close all VDP reports determined to be duplicates or out-of-scope.

The contractor shall close any VDP reports where the reported vulnerability has been determined by the system owner to be an accepted risk, or where the vulnerability is pending mitigation per an approved Plan of Action and Milestones (POA&M).

The contractor shall recommend closing appropriate VDP reports that are informative but not requiring further action and shall recommend referral of VDP reports to other Government agencies as appropriate. If new VDP reports do not provide sufficient detail for the contractor to make these assessments, the contractor shall identify the deficiency and communicate this information to the reporting researcher.

VDP report management workflow duties require specialized knowledge of various tools, such as but not limited to, Kali Linux, Burp Suite, and Whois databases.

The contractor shall be responsible for twice daily report synchronization between NIPRNET and SIPRNET Vulnerability Report Management Network (VRMN) instances.

The contractor shall assess vulnerabilities reported under the VDP to validate the information provided by the private-sector researchers. The contractor assessment shall include replicating the actions taken by the researchers to identify the reported vulnerability. If additional information is required to validate the reported vulnerability, the contractor shall determine and document the additional information needed from the researcher to conduct this assessment. The contractor shall identify VDP reports with confirmed vulnerabilities for mitigation action by the affected customer.

The contractor shall use various open-source tools (e.g., Kali Linux, Burp Suite, browser development tools) as required.

The contractor shall identify VDP reports with vulnerabilities that cannot be validated and shall provide recommendations for disposition of these VDP reports.

SECTION C – PERFORMANCE WORK STATEMENT

C.5.6.2 SUBTASK 6.2 – IDENTIFY SYSTEM OWNERS

The contractor shall review the DoD Demilitarized Zone (DMZ) Whitelist to determine the owners of systems with vulnerabilities identified by VDP reporting. For systems identified in the DMZ Whitelist, the contractor shall document all detailed organizational/individual contact information so that it can be provided to Joint Force Headquarters (JFHQ)-DoDIN to facilitate tasking to the appropriate DoD Component. This information shall also be provided to the DISA so that they may update the DMZ whitelist.

For systems that cannot be identified in the DMZ Whitelist, the contractor shall use available information to identify and contact system owners.

The contractor shall establish and maintain a separate list of all DoD managed websites and web applications that are not on the DoDIN.

C.5.6.3 SUBTASK 6.3 – IDENTIFY RELEVANT VULNERABILITY GOVERNANCE

The contractor shall review validated VDP reports to identify existing DoD CS governance relevant to the reported vulnerability.

The contractor shall identify specific Security Technical Implementation Guides (STIGs) and/or RMF security controls that may be relevant to the reported vulnerability. This information will be documented so that it can be provided to JFHQ-DoDIN to facilitate mitigation actions by the affected Component.

C.5.6.4 SUBTASK 6.4 – TRANSMIT VALIDATED VDP REPORTS TO JFHQ-DoDIN

The contractor shall assign validated VDP reports with validated vulnerabilities to JFHQ-DoDIN to facilitate tasking to the appropriate DoD Component.

The contractor shall integrate the initial VDP report from the researcher; report and vulnerability validation results; system owner contact information; and relevant governance documentation for transmittal to JFHQ-DoDIN via the VRMN platform. The contractor shall verify receipt of the report package by JFHQ-DoDIN.

C.5.6.5 SUBTASK 6.5 – COORDINATE OPEN VDP REPORTS WITH PRIVATE-SECTOR RESEARCHERS AND DOD COMPONENTS

The contractor shall maintain appropriate communication with private-sector researchers, JFHQ-DoDIN, and DoD Components on all open reports IAW the VDP CONOPS.

The contractor shall ensure inquiries, updates, and other communications are promptly and properly coordinated with all appropriate parties to maintain shared situational awareness on the processing and status of VDP reports.

C.5.6.6 SUBTASK 6.6 – VALIDATE REPORTED MITIGATION ACTIONS

The contractor shall assess actions taken by DoD system owners to validate that any vulnerabilities reported by private-sector researchers under the VDP are effectively mitigated. The contractor assessment shall include replicating the actions taken by the researchers to determine if the reported vulnerability has been mitigated. The contractor shall mark as resolved

SECTION C – PERFORMANCE WORK STATEMENT

and recommend closure of VDP reports with mitigated vulnerabilities and will recommend returning reports with unmitigated vulnerabilities to JFHQ-DoDIN for further action.

C.5.6.7 SUBTASK 6.7 – RETURN REPORTS WITH UNMITIGATED VULNERABILITIES TO JFHQ-DoDIN

The contractor shall return VDP reports with unmitigated vulnerabilities to JFHQ-DoDIN via VRMN to facilitate re-tasking to the appropriate DoD Component. The contractor shall include the steps and results of the assessment conducted which determined the vulnerability was still present. The contractor shall confirm receipt of the returned VDP report package by JFHQ-DoDIN.

C.5.6.8 SUBTASK 6.8 – CLOSE REPORTS WITH MITIGATED OR ACCEPTED VULNERABILITIES

The contractor shall close VDP reports with mitigated vulnerabilities and notify the researcher. The contractor shall also close VDP reports and notify the researcher if the system owner has accepted the risk of an unmitigated vulnerability or has an approved POA&M to mitigate the vulnerability at a later date.

C.5.6.9 SUBTASK 6.9 – AFTER-ACTION ASSESSMENT

The contractor shall develop an after-action assessment to be completed by owners of DoD systems with validated vulnerabilities. The contractor shall collect, aggregate, and analyze the information provided by the system owners to identify gaps in DoDIN defenses, areas requiring increased attention, and areas for improvement. The contractor shall publish a monthly and annual report documenting the results of these assessments and include recommendations to improve DoDIN defenses.

C.5.6.10 SUBTASK 6.10 – FOLLOW-UP ON MISSING AND INCOMPLETE AFTER-ACTION ASSESSMENTS

The contractor shall follow-up on missing and incomplete after-action assessments through JFHQ-DoDIN via VRMN to obtain the after-action assessment from the appropriate DoD Component. The contractor shall confirm receipt of the completed after-action assessment from JFHQ-DoDIN.

C.5.6.11 SUBTASK 6.11 – COLLECT AND REPORT PROGRAM METRICS

The contractor shall capture, aggregate, analyze, and report program process and performance measures. The contractor shall collect, analyze, and report data, which includes, but is not limited to, the following proposed metrics:

Vulnerability Lifecycle/Process Metrics

- a. Median triage time.
- b. Median remediation time.
- c. Median component remediation time by component.
- d. Median component remediation time per month.
- e. Median component remediation time by type of vulnerability.
- f. Median component remediation time by severity of vulnerability.

SECTION C – PERFORMANCE WORK STATEMENT

Security Controls Metrics

- a. To identify compliance issues:
 1. Percent of vulnerabilities covered by existing STIGs, IAVA/Bulletin (IAVA/Bs), Orders, or Common Vulnerabilities and Exposures (CVEs).
 2. Number Vulnerabilities per existing STIG, IAVA/B, Order, or CVE: JFHQ-DoDIN.
- b. To identify trends and drive future orders:
 1. Types of root-causes reported by components.
 2. Percent of Vulnerabilities not covered by existing controls.
 3. Vulnerabilities not covered by existing controls (broken out by reported root-cause).

Vulnerability Statistics

- a. Total number of reports
 1. Broken out per month by total, open, closed, resolved, duplicate.
 2. Broken out by component.
- b. Types of validated vulnerabilities
 1. Number per month.
- c. Severity of validated vulnerabilities
 1. Number per month.
 2. Median severity over time.

The contractor shall capture, aggregate, analyze, and report TO performance measures. Key metrics gathered will be used for Performance Management Workflow to establish measurement and analysis continuity as well as to cover Government-requested reports and DoD CIO scorecards/dashboards and published monthly performance reports for dissemination to VDP stakeholders. The contractor shall gather aggregated metrics for annual reporting.

C.5.6.12 SUBTASK 6.12 – MAINTAIN VULNERABILITY REPORT MANAGEMENT NETWORK (VRMN)

The contractor shall maintain the VDP VRMN system, a JIRA-based or similar platform, to sustain capabilities delivered by the successful execution of the VDP mission. This includes, but is not limited to, software and hardware fixes and any necessary upgrades coordinated with the BTO ITD Chief. Major upgrades to the system that deliver new capabilities will be managed as separate subtasks.

C.5.6.13 SUBTASK 6.13 – VRMN CONTINUOUS DEVELOPMENT

The contractor shall provide continuous development of VRMN. High-level requirements for this system include, but are not limited to:

- a. Identification and management of new system requirements.
- b. Import/export of new and changed data from the private crowd-sourced bug bounty hosting organization(s) system and data migration to the system on SIPRNET.

SECTION C – PERFORMANCE WORK STATEMENT

- c. Identification and documentation of system owners.
- d. Identification and documentation of relevant IAVAs, STIGS, and RMF controls.
- e. Dissemination of VDP reports and attachments to JFHQ-DoDIN, the components, and system owners.
- f. Tracking the status of VDP reports as they are processed, disseminated, and resolved.
- g. Capture and reporting of after-action Assessment data.
- h. Capture and reporting of metrics data for DoD CIO.
- i. Integration with various third- party tools, Application Programming Interfaces (APIs), and databases.
- j. Expansion of access down to the system-owner level.
- k. Management of the VRMN FAQ.
- l. VRMN server maintenance scheduled to avoid stakeholder impact.

C.5.6.14 SUBTASK 6.14 – VDP QA AND TRAINING

The contractor shall build, maintain, and execute a rotating target list of DoD assets that will be tested against using industry practices to find and report vulnerabilities found in DoD public-facing assets. The desired benefits are threefold:

- a. Ensure previously reported critical vulnerabilities are still mitigated.
- b. Further test known “chronically vulnerable” systems to improve cyber hygiene.
- c. Maintain the contractor’s technical competencies, capabilities, and skills.

This type of active vulnerability hunting shall be done during downtime and/or gaps of activity for the third-party research community.

- a. Create target lists.
- b. Update target lists.
- c. Rotate target lists as needed.
- d. Create lessons learned and case studies on findings.
- e. Produce whitepapers from findings.

C.5.7 TASK 7 - ENTERPRISE MANAGEMENT & RESOURCING (ER) SUPPORT

The contractor shall support all functions of DC3’s ER Directorate. Those functions are outlined in the proceeding subtasks.

C.5.7.1 SUBTASK 7.1 – DC3 PLANNING, PROGRAMMING, EXECUTION, AND BUDGET SUPPORT

The contractor shall research, analyze, and evaluate data from existing manpower and budgetary databases (i.e., Automated Budget Interactive Data Environmental System (ABIDES), interlink Resource Management Information System (iRMIS)), Congressional Records, DoD, U.S. Unified and Specified Commands, and AF operational commands to develop optimum investment strategies for DC3 consideration.

The contractor shall assist in the formulation of and monitor the execution of long-range detailed budget forecasts, financial plans, and five-year programs to fund implementation of substantive

Task Order 47QFCA22F0025

Modification P00001

PAGE C-31

SECTION C – PERFORMANCE WORK STATEMENT

cyber programs and projects. This assistance shall not include the determination of DC3 program priorities for budget requests. The contractor shall conduct detailed research of budget forecasts and execution histories from a number of highly technical cyber programs to identify trends, anomalies, and potential capability gaps.

The contractor shall analyze guidance for multi-year appropriations to identify resource shortfalls and offsets, prepare appropriate supporting documentation, and identify alternative methods of financing unfunded requirements. The contractor shall maintain DC3 information in manpower, programming, and budgeting databases as well as providing timely and accurate response to inquiries and taskings pertaining to DC3 planning, programming, and budgeting.

C.5.7.2 SUBTASK 7.2 – DC3 PROGRAM MANAGEMENT OFFICE (PMO)

The contractor shall assist in establishing and maintaining DC3 portfolio management capability by developing, implementing, monitoring, and supporting processes and tools in the following subjects to include but not limited to: baseline change control, risk, issues, and opportunities, project finance, schedule management, requirements and project prioritization management (**Section F, Deliverable 30**).

The contractor shall develop and maintain the DC3 Enterprise baseline and forecast resource-loaded Integrated Master Schedule (IMS) utilizing MS Project (2013 or later). The contractor shall support the Government with schedule analysis, identifying root causes to variance, creating and presenting cost and schedule metrics. The contractor shall provide industry best practices as it relates to program management tools, process, and PMO structure.

C.5.8 TASK 8 – BUSINESS & TECHNOLOGY OPERATIONS (BTO) SUPPORT

The contractor shall support DC3 business operations by providing administrative support, security, logistics, human resources, policy development, policy administration, strategic planning, exercise planning, agreement management, CS, enterprise architecture, IT portfolio management support, intellectual property management, technology transfer support, partnership liaison and facilities. These shared services enable each of the Directorates to focus on delivery of its core mission and maintain a common operational support mechanism.

C.5.8.1 SUBTASK 8.1 – IT ENVIRONMENT AND SERVICE DESK SUPPORT

The contractor shall provide assistance to DC3's IT infrastructure, telecommunications requirements, and service desk. The ITD requires on-call contractor support to maintain 24 hours per day, seven days per week, 365 days per year (24x7x365) operational availability of critical networks and systems. The ITD is currently responsible for 12 separate networks and telecommunications systems of all classification levels serving more than 400 users throughout the DC3 organization. ITD critical networks and systems currently consist of the Unclassified DEN, Classified SDEN, DC3ON, DC3/CFL Networks (ExLAN, IA LAN), and phone systems. The ITD also maintains and supports all Corporate and Forensics applications that run on forensically sound workstations, several of which are mission critical.

DC3's IT services are maintained IAW all DoD and AF directives, guidelines, and requirements such as (but not limited to) DoDD 8570, DoDD 8140, AFMAN 17-1303, and AFMAN 17-1301.

SECTION C – PERFORMANCE WORK STATEMENT

DC3 operates and maintains two non-classified networks: NIPRNET DEN and DC3ON; two SIPRNET networks, SDEN and DC3's Classified Secure Automated Data Obfuscation Network, one JWICS network, a closed Special Access Program (SAP) network, and multiple stand-alone forensic/examination networks that provide processing and communications support.

The NIPRNET provides seamless interoperability for unclassified combat support applications, as well as controlled access to the Internet. SIPRNET is DoD's largest interoperable command and control data network, supporting the Global Command and Control System (GCCS), the Defense Message System (DMS), collective planning, and numerous other classified warfighter applications.

The Service Desk is the single POC for all DC3 requests for service including computer user and telecommunications-related issues. The Service Desk supports the Linthicum, Maryland locations. In 2019, ITD received 6,728 calls/requests. The requests are generally resolved via first call resolution; however, technicians may be required to be dispatched to troubleshoot and provide immediate resolution to the problem. The issues occur based on various security classifications levels, to include Controlled Unclassified Information (CUI), Secret, TS, SCI, SAP, and Special Access Required (SAR). All technicians performing network functions (as defined in AFMAN 17-1303 or later version) shall be Information Assurance Technical (IAT) Level II or higher certified IAW DoDD 8570.01 and 8140.01.

The contractor shall provide Tier 0 (self-service), Tier 1, and 2 service desk support for all DC3 computer users. This activity includes requests for installation, repairs, and upgrades of existing equipment. The contractor shall provide personnel onsite daily to respond to technical support issues from 6:00 am through 6:00 pm Eastern Standard Time (EST) on a 12 hours per day, five days per week basis (Monday through Friday). The contractor is required to provide on-call support (outside of the standard working hours) for unplanned events.

The contractor shall develop the Tier 0 or self-service mechanism to support DC3 computer users. The contractor shall provide a technical Tier 1 service desk (initial caller support) for DC3. Tier 1 is the first point of customer contact for network related operational issues. Typical Tier 1 support includes, but is not limited to, requests related to COTS hardware failures, software failures, application questions, installations, relocations, turn-ins, access rights, hardware/software loaners, network communication failures, new user requirements, temporary computer product check-outs, and other computer related requirements. All issues beyond the capabilities of Tier 1 caller support are escalated to Tier 2 or Tier 3.

The contractor shall provide Tier 2 service desk technical support for DC3 user issues. The contractor shall serve as the SME for troubleshooting desktop support related issues. The contractor shall design, troubleshoot, and implement DC3 computer-related equipment. In addition to Tier 2 troubleshooting, the contractor shall:

- a. Identify network problems due to design and implementation constraints.
- b. Identify and implement workarounds to resolve DC3 network problems.
- c. Work with DC3 network design engineers on engineering and design issues to develop operationally sound implementations.

SECTION C – PERFORMANCE WORK STATEMENT

- d. Develop troubleshooting guides and SOPs to improve Tier 0 and enable Tier 1 technicians to efficiently troubleshoot and resolve DC3 network problems (**Section F, Deliverable 31**).

The contractor shall respond to and document all network incidents including security and informational requests that result from proactive network monitoring or customer-initiated contacts. The contractor shall isolate and document network problems using industry best practice troubleshooting skills, as well as available system and network management tools. The contractor shall use the current or recommend a new equivalent Service Desk Ticket application (currently Jira) as a central repository for technical advice and solutions for IT systems, software applications assistance, automatic data processing support, hardware exchange, repair service support, and other related service desk functions.

The contractor shall utilize network management tools to provide efficient, responsive, and rapid problem resolution.

The contractor shall collect and report IT service desk service performance metrics. The contractor, as a minimum, shall establish and maintain metrics (subject to Government approval) of the following items, and be prepared to present the findings to DC3 leadership:

- a. Total number of queries into the ITD.
- b. Total number of queries into the ITD that result in a trouble ticket (separated by category such as, incidents, problems, requests for change, and requests for services).
- c. Total number of queries that are resolved during initial contact.
- d. Total number of queries resolved by the ITD.
- e. Total time to complete (resolve) the trouble ticket.

At a minimum, the contractor shall respond to customer service desk requests within four hours and complete resolution within 24 hours (during regular business hours Monday through Friday 6:00 am through 6:00 pm EST). The contractor shall provide supporting documentation for validation by the DC3 for those requests beyond the desired response and resolution periods. The contractor shall track all service desk requests from inception through completion in the service desk ticketing system.

The contractor shall provide Monthly Service Desk Trouble Call Status Reports (TCSRs) (**Section F, Deliverable 32**). The contractor shall provide Service Desk TCSRs that provide relevant data and reports on information such as:

- a. Analyses/type of trouble calls.
- b. Unusual patterns.
- c. Potential DC3 IT/Communications/application problems and proposed resolutions.
- d. Unresolved Trouble Tickets.
- e. Tracking and resolution of service complaints.
- f. Backup source data.
- g. Summary status (in spreadsheet format) of all hardware maintenance for each month.

SECTION C – PERFORMANCE WORK STATEMENT

C.5.8.2 SUBTASK 8.2 – NETWORK AND SYSTEMS ADMINISTRATION SUPPORT

DC3 relies upon the following networks (currently 12 in total) and their associated services for its daily operations and mission support:

- a. DEN NIPRNET (supporting approximately 450 users).
- b. SDEN SIPRNET (supporting approximately 250 users).
- c. JWICS (supporting approximately 200 users).
- d. DC3's (internal) Laboratory Information Management System (CIMS10), Forensic Examiner, and Intrusion Networks.
- e. DC3ON.
- f. Automated Data Obfuscation Classified Network Enclave.
- g. Covered Accounts Network.
- h. Virtual Private Network (VPN) on unclassified networks.
- i. Other networks as required by the Government.

The contractor shall ensure identified networks and IT (currently DEN, SDEN, DC3ON, and Defense Industrial Base Local Area Network (DIBLAN)) align with the complete Risk Management Framework (RMF) and successfully obtain and maintain Authority to Operate (ATO).

The contractor shall install and maintain routers, switches, hubs, and cabling comprising DC3's network infrastructure. The contractor shall maintain the IP addressing schema for the entire enterprise infrastructure; modify switch, router, and hub configurations to ensure optimum network performance; and configure Access Control Lists (ACLs) to grant/restrict network access to authorized users and protocols.

The contractor shall provide proactive and reactive management of resources by monitoring and controlling networks, available bandwidth, hardware, and distributed software resources.

The contractor shall operate and maintain the aforementioned networks to include, but are not limited to, the following tasks:

- a. Install, configure, manage, troubleshoot, and secure network infrastructure, including but not limited to servers, storage components, desktop computers (PCs), laptops, printers, scanners, routers, switches, network devices, and other tools.
- b. Design and configure network components, including VPN capabilities.
- c. Monitor and manage network bandwidth.
- d. Perform back-up and recovery functions.
- e. Establish, monitor, and maintain all computer and network accounts (Add/Change/Deletion) IAW DoD, AF, and DC3 BTO/ITD computer security regulations.
- f. Maintain the Global Address List, Active Directory and other network directory services.
- g. Maintain an up-to-date listing of user accounts, email accounts, passwords, software licenses, systems file directories, and system/network accreditation documentation.
- h. Operate, maintain, and trouble-shoot video teleconferencing hardware and software

SECTION C – PERFORMANCE WORK STATEMENT

- i. Manage internet and intranet web servers, remote Access Security Services, and maintain the Domain Name System (DNS) server.
- j. Maintain and monitor standardized file storage directory structures.
- k. Establish, maintain, and monitor print servers.
- l. Coordinate with third party organizations and network carriers to perform operational activities.
- m. Develop and document network administration policies and procedures.
- n. Document and report all network faults, outages, and security incidents.
- o. Document and maintain enterprise user account information.
- p. Conduct analysis of network characteristics to include traffic, connect time, transmission speeds, packet, and modifications to network and system components.
- q. Recommend processes and tools to improve overall network performance and user experience.

All technicians performing network and IT functions (as defined in AFMAN 17-1303 or later version) shall be, at a minimum, IAT level II certified IAW DoD 8570.01 and DoD 8140.01.

DC3 is currently moving its existing infrastructure to a thin client and virtual environment with an objective state of using cloud services both on premise and off-premise. The contractor shall provide planning, implementation, and maintenance support for all new infrastructure changes, phases, or surge efforts as required.

The contractor shall also make recommendations to the Government for upgrades, equipment replacement, repairs, changes, additions, and removal of parts of DC3 IT infrastructure. The contractor shall notify the Government of all required changes, additions or removals from the existing system and obtain concurrence before any changes, additions, or removals are performed. DC3 has a configuration control process to document and approve all changes to the IT services baseline. The contractor shall ensure all changes are IAW this process and conform to established policy and standards. The contractor shall document all repairs, changes, additions, or removals in the summary status included in the TCSR. The contractor shall conduct technical testing on existing and newly procured ITD systems, subsystems, and applications.

The contractor shall evaluate communications hardware and software, troubleshoot problems, and provide technical expertise for optimal performance of equipment. The contractor shall recommend additional hardware and software tools, which could improve the systems. The contractor shall ensure that DC3's networks, applications, and systems maintain at a minimum a monthly 99.5 percent network/systems availability.

The contractor shall notify the Government of any unusual circumstances that exist beyond the contractor's control for not meeting the availability service levels. The contractor is required to monitor, maintain, track, record, and report monthly system availability, up time, and downtime. The contractor shall provide this information to the Government on-demand.

In the event that network connectivity/availability is caused or impacted by an external source (i.e., not DC3), the contractor shall ensure the ITD Director, CISO, BTO Director/Chief Information Officer (CIO), and DC3 TPOC are notified, in writing, within 30 minutes of the

SECTION C – PERFORMANCE WORK STATEMENT

incident (during regular business hours Monday through Friday, 6:00 am through 6:00 pm EST). This report shall include the cause and anticipated restoration time.

The contractor shall ensure all network incidents are identified in the MSR with descriptions of the incident, causes, resolutions, and any Government actions required. The contractor shall ensure this information is made available, on demand, to the Government.

The contractor shall respond to detected security incidents, network faults (errors), and user reported outages within 30 minutes of notification of an incident. The contractor shall notify the Government (CISO, ITD Director, BTO Director/CIO, and DC3 TPOC) within 30 minutes of any security incident or network outage (during regular business hours Monday through Friday, 6:00 am through 6:00 pm EST, incidents outside of business hours shall be reported by 6:30 am EST the next business next day).

The contractor shall document, record, and report all network incidents and include these within the MSR.

C.5.8.3 SUBTASK 8.3 – ENTERPRISE ARCHITECTURE (EA)

DC3's EA conforms to the DoD Joint Information Environment (JIE), which consists of five major focus areas: optimization of information, network, hardware, applications, and governance. Each of these capabilities is described in terms of activities⁵¹, services, and rules necessary to ensure the capability is achieved. The DoD Information Environment Area (IEA) outlines how capabilities are delivered by providing descriptions of services the DoD IEA must have to operate at optimum effectiveness. These services represent a collection of required information across the spectrum of Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P).

The contractor shall develop and maintain the baseline artifacts of the following views: AV-1, AV-2, CV-1, CV-2, CV-6, CV-7, OV-1, OV-5a, OV-6a, SvcV-1, SvcV-4, StdV-1, and StdV-2 (**Section F, Deliverable 33**). Furthermore, the contractor shall provide documentation IAW DC3 standards to substantiate the DC3 current and future states as the DC3 architecture evolves. The contractor shall be responsible for requirements analysis, evaluation, and design of the IT architecture environment for DC3.

The contractor shall maintain a current EA and configuration design for all DC3 networks. The contractor shall provide DC3 with a well-defined practice for conducting enterprise analysis, design, planning, and implementation, using a holistic approach at all times, for the successful development and execution of strategy.

The contractor shall apply DoD/AF architecture principles and practices to guide the DC3 through the business, information, process, and technology changes necessary to execute its strategies and objectives.

C.5.8.4 SUBTASK 8.4 – CONFIGURATION MANAGEMENT (CM)

The contractor shall develop, implement, and support DC3's Configuration Management (CM) processes for all networks and supporting technologies identified in this PWS (**Section F, Deliverable 34**). The DC3 CM shall consist of a systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with

SECTION C – PERFORMANCE WORK STATEMENT

its requirements, design, and operational information throughout its life. This shall include assurance of adequate CM software that tracks and controls changes in any DC3 IT, software, or application, thereby maintaining strict accounting of the DC3 IT services baselines. The contractor shall not make any unauthorized changes to the baseline without the express approval of the Government CISO and either the Chief of ITD or the DC3 CIO.

The CM system process shall include configuration identification, data management, audits, change control, status accounting, and deficiency reporting. The CM system/process shall be documented in a Configuration Management Plan (CMP) (**Section F, Deliverable 35**) that includes/addresses the entire IT lifecycle.

The contractor shall support the installation and configuration of network servers, routers, and other peripherals. The contractor shall be responsible for CM design, architecture, and COTS/GOTS software and hardware integration including, but not limited to, describing provisions for configuration identification, configuration of requirements documentation, design documentation, software, and related documentation.

The contractor shall be responsible for configuration change control, configuration status accounting, and configuration audits. The contractor shall regulate the change process so that only approved and validated changes are incorporated into product documents and related software. The contractor shall track and report all CM problems and support software quality assurance process audits.

The contractor shall evaluate, implement, and configure hardware and software to ensure AF Information Protection (AFIP) and DoD policies are enforced, and safeguards are active.

The contractor shall configure test beds to conduct testing on DC3 networks, record and analyze results, and provide recommendations for improvements of the products/systems tested. The contractor shall encode, debug, and test software applications to meet established operational and system requirements using industry standard products such as programming languages and tools.

C.5.8.5 SUBTASK 8.5 – IT ASSET MANAGEMENT

The contractor shall provide support in receiving, tracking, distributing, and accounting for DC3's hardware and software inventory. DC3 currently uses Jira and DPAS for its asset management lifecycle accounting.

The contractor shall maintain an up-to-date library of all major equipment warranty/maintenance contract information as well as lifecycle and End of Life (EOL) status.

The contractor shall maintain a complete inventory of all of DC3's major hardware and/or designated components and the recording of serial numbers and related nomenclature. The contractor shall maintain and update a software library accounting for all software, licenses, and issuance data. The contractor shall ensure all asset lifecycle information is tracked, monitored, and reported appropriately to ensure timely renewal or refresh of EOL assets.

The contractor shall document and regularly update the Total Cost of Operations (TCO) for each DC3 network IAW guidelines provided by the Government. To identify costs as well as provide investment transparency, the contractor shall assist the Government in developing a chargeback or show back model that depicts IT investments by identifying the components of IT costs that are directly associated to the infrastructure, data transfer, application licenses, and training,

Task Order 47QFCA22F0025

Modification P00001

PAGE C-38

SECTION C – PERFORMANCE WORK STATEMENT

which they generate. The intent is to ensure appropriate use of IT resources, provide visibility to the DC3 leadership, substantiate rationale for IT decisions, and conform to budgeted IT services.

The contractor shall ensure IT asset information is made available to the Government, on demand.

C.5.8.6 SUBTASK 8.6 – CYBERSECURITY (CS)

The contractor shall assist in maintaining CS protection of all DC3 data and systems. The contractor shall provide technical support to maintain the confidentiality, integrity, and availability of data and privacy of DC3 IT and mission information systems.

The contractor shall support the DC3 CISO in executing the CS requirements for DC3 information technologies through the use of the RMF consistent with the principles established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37r2 and as outlined in DoDI 8510.01, RMF for DoD IT. The contractor shall perform continuous monitoring activity and support the implementation and operations of an insider threat mitigation capability. The contractor shall continually identify and inject RMF requirements into DC3 acquisition processes, requirements development, procurement, and IT (hardware and software) development efforts.

The contractor shall provide services to include proactive security vulnerability assessment, implementation, and monitoring of all computer systems and network infrastructure. The contractor shall perform vulnerability/risk analyses of computer/network systems and applications during all phases of the system development lifecycle. The contractor shall assist in conducting certification and accreditation on applications IAW the RMF.

The contractor shall assist in mitigating the threat of network intrusions by proactively probing network defenses to identify vulnerabilities to include administering network scans.

The contractor shall ensure the latest security updates are enforced, ensure Information Assurance Vulnerability Alert (IAVA) and Tactical Computer Network Operator (TCNO) compliance, and provide real-time protection from any threats of active files using anti-virus tools. The contractor shall operate and maintain firewall(s), web proxies, caching servers, and email gateway servers to protect DC3 information resources from internal and external threats. The contractor shall ensure all current network security tools and patches are implemented across all internal DC3 systems IAW AF and DoD standards. The contractor shall conduct daily security scans of computer/network systems and advise the Government of potential computer security concerns and problems along with recommendations for solutions.

The contractor shall develop/maintain measures and controls to protect the DC3 networks from denial of service, unauthorized access, and modification of data and destruction of DC3 networks, network components, or information processed on them. The contractor shall document and maintain IT security policies, procedures, and awareness.

The contractor shall perform information protection functions for networks and IT systems. The contractor shall test computer/network systems and applications for the following:

- a. Ease of unauthorized entry.
- b. Systems resources denial.

SECTION C – PERFORMANCE WORK STATEMENT

- c. System information corruption.
- d. Unlawful use of system resources.
- e. Vulnerability to electronic disruption.

The contractor shall report and document all identified system attacks to the CISO, DC3 BTO Director/CIO, and DC3 TPOC.

The contractor shall provide support related to COMSEC. The contractor shall document receipt, custody, issuance, transmittal, storage, accountability, classification, and destruction of all Classified Material. The contractor shall maintain logs and journals to comply with AF security, regulatory, and policy guidelines. The contractor shall be responsible for maintaining and updating all secure equipment, records, and self-inspection programs concerning Classified Material.

The contractor shall ensure all systems and equipment are operated and maintained IAW DoD; Defense Information Systems Agency (DISA); USAF; Secretary of the AF/Inspector General (SAF/IG); and OSI security guidelines, directives, and updates. The contractor shall ensure all security policies are within the limits of existing architecture and software capabilities. The contractor shall ensure the DC3 network and IT systems are 100 percent in compliance with applicable DoD and USAF directives for Network and Computer Security.

C.5.8.7 SUBTASK 8.7 – WEB, PORTAL, AND CONTENT MANAGEMENT SYSTEM (CMS) DEVELOPMENT AND MANAGEMENT

The contractor shall support the DC3 internet and intranet websites, collaborative portals, and CMSs supported by this order. The contractor shall provide administrative, development, and technical management of all facets of the managed websites, portals, and CMSs as required for the Government's review and approval.

The contractor shall keep all content on managed DC3 websites/portals current. This content includes a running inventory of these information outlets and their information owners. The contractor shall ensure all content is compliant with DoD and USAF policies, directives, and standards. The Government PAO must approve all public facing information.

The contractor shall provide a review of all content updates at each MSR. The contractor shall perform continual evaluations of websites, portals, and CMS software and hardware to ensure continued and future effectiveness and efficiency of these capabilities and recommend updates, changes to the Government as appropriate and necessary.

The contractor shall design, develop, and implement web pages that fully comply with AF/DOD/DC3/PAO requirements and standards (**Section F, Deliverable 36**). The contractor shall maintain DC3's World Wide Web (WWW), NIPRNET, SIPRNET, Portal, and JWICS websites and content.

C.5.8.8 SUBTASK 8.8 –DATABASE MANAGEMENT SUPPORT

Data management is the practice of collecting, keeping, and using data securely, efficiently, and cost-effectively. The goal of data management is to facilitate DC3 to optimize the use of data within the bounds of policy and regulation so that it can make decisions and take actions that maximize the benefit to the organization. Managing digital data in an organization involves a

SECTION C – PERFORMANCE WORK STATEMENT

broad range of tasks, policies, procedures, and practices. The scope of data management can include the following tasks:

- a. Create, access, and update data across a diverse data tier.
- b. Store data across multiple clouds and on premises.
- c. Provide high availability and disaster recovery.
- d. Use data in a growing variety of apps, analytics, and algorithms.
- e. Ensure data privacy and security.
- f. Archive and destroy data IAW retention schedules and compliance requirements.

The contractor shall assist the Government with a formal data management strategy that addresses the activity of users and administrators, the capabilities of data management technologies, the demands of regulatory requirements, and the needs of the organization to obtain value from its data.

The contractor shall provide database installation, configuration, and management for all DC3 databases. The contractor shall perform incremental daily backups and weekly full backups. The contractor shall ensure that information from the databases is accessible to users as determined by the Government, using documented instructions provided by the contractor. The contractor shall develop and administer security procedures to ensure only valid users have access to data and data modification. The contractor shall be responsible for ensuring data integrity while performing database related functions.

C.5.8.9 SUBTASK 8.9 – VIDEO AND TELECOMMUNICATIONS SUPPORT

The contractor shall provide over all support to DC3's telephone, telecommunications systems, and secure telecommunications equipment (currently Voice over Internet Protocol (VoIP) and Private Branch Exchange (PBX)). The contractor shall provide day-to-day technical administration of the phone system, perform scheduled and non-scheduled maintenance, coordinate repair actions with service providers, and verify telecommunications circuits are active and available for use. The contractor shall monitor the performance of telephone sets, voicemail systems, modems, fiber optic cables, telephone switching units, and data circuits.

The contractor shall provide immediate written notice within 24 hours to the DC3 ITD Director, BTO Director/CIO, and DC3 TPOC of a situation impacting communications. The contractor shall provide end-user training for telephone devices to support voicemail configuration, and all other phone system operations and features. The contractor shall provide onsite technical support for Audio-Visual (AV) and Video Conferencing equipment (currently Tandberg) for multiple classification levels (NIPR, SIPR, and JWICS.)

C.5.8.10 SUBTASK 8.10 – CLOUD MIGRATION

The contractor shall perform a complete review of existing or To-Be DC3 Azure cloud landscape and provide suggested Courses of Action (COAs) and improvements based on Azure Cloud best practice and DoD Cloud Security Requirements Guide (SRG) on the below areas during the DC3 Azure Cloud standup and application migration:

Core cloud configurations, standards, and governance:

SECTION C – PERFORMANCE WORK STATEMENT

- a. Review DC3 cloud platform governance services, their use, and configuration best practices.
- b. Perform account planning and overall billing structure review.
- c. Provide advisement around a subscription creation strategy to support dev, test, and operational environments.
- d. Provide advisement on tagging and billing strategy.
- e. Provide advisement on resource group approach.
- f. Provide advisement on naming standards that are in line with current enterprise requirements.
- g. Provide advisement on governance framework utilizing Management Groups, Azure Policies and Resource Locks and implement best practice privileged account access approach using Multi-Factor Authentications (MFAs).
- h. Review cost containment best practices to develop strategy and identify cost containment tools.

Identity Access Management (IAM)

- a. Review identity, access management requirements, and discuss overall integration approach.
- b. Propose possible approaches to achieve advanced services such as Single Sign On (SSO) and MFA integrating with existing SaaS offering (e.g., Salesforce).
- c. Identify any third-party tool integration requirements and provide integration guidance.
- d. Perform review of roles, groups, accounts, and security policies required to support role-based access control requirements and advise on implementation.
- e. Review network and interconnectivity between DC3 on premises networks and Azure platform.
- f. Review cloud platform network and interconnectivity services, their use, and configuration best practices.
- g. Identify regions, network segmentation, traffic flow management, and routing requirements.
- h. Identify the need for any network appliances and where they are integrated into design.
- i. Review the implemented common network services such as DISA Secure Cloud Computing Architecture (SCCA), Content Delivery Network (CDN), load balancing, application gateways or web application firewall appliances and provide any enhancement or future implementation advisement.
- j. Determine interconnectivity technologies and provide guidance around best practices.

Security:

- a. Review cloud platform native security services, their use and configuration best practices (e.g., Sentinel, Azure Defender, Azure Security Center, and Azure Advanced Threat Protection (ATP)).
- b. Determine compliance requirements and security services required.
- c. Identify and advise on third-party security services required to meet security requirements.

SECTION C – PERFORMANCE WORK STATEMENT

- d. Provide guidance around logging, auditing, and alerting strategy.

Operational Readiness:

- a. Review operational best practices, capabilities, and approaches to integrate the Azure environment into current operational processes.
- b. Advise on operational best practices regarding alerts and monitoring.
- c. Provide background on automated response and provisioning, operational analytics, and machine learning capabilities available within Azure.

Design Whiteboarding:

- a. Perform interactive sessions with the customer to whiteboard possible design improvements.
- b. Work through possible best practices improvements and designs using the information obtained from the customer.
- c. Discuss industry trends, other DoD customer implementations around DoD cloud designs, and implementations.
- d. Review existing application and infrastructure landscape and discuss possible improvements around resiliency and scalability utilizing Azure PaaS and SaaS offerings (e.g., Azure Kubernetes Service (AKS) and Serverless computing).

Disaster Recovery and Backup Strategy:

- a. Review existing Disaster Recovery and backup landscape and processes to provide best practices and capabilities for Azure hybrid cloud landscapes.
- b. Provide deep knowledge transfer around Azure disaster recovery and backup services, their configurations, and optimal usage techniques.
- c. Review current On Premise storage usage and recovery practices to determine most effective backup landscape components.
- d. Discuss backup policies, retention, and archival processes for optimal cloud usage and help configure Cohesity Cloud backup solution accordingly in Azure.
- e. Review current disaster recovery approach, processes, technology tools, and physical landscape.
- f. Discuss data replication and availability approaches to support backup and disaster recovery operations.
- g. Advise on possible approaches to achieving application and infrastructure resiliency that meet overall Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets.

DevSecOps in Azure:

- a. Recommend DevOps pipelines in support of DC3 CI, Continuous Deployment, Infrastructure-as-Code and related DevOps, Security, and Automation for application developers' needs (e.g., Platform One Customer DevSecOps Platform (DSOP)).
- b. Provide the adoption strategy migrating current On Premise DevOps pipelines to Cloud-Native software solution development, integration, testing, and deployment, with seamless visibility and traceability.

Task Order 47QFCA22F0025

Modification P00001

PAGE C-43

SECTION C – PERFORMANCE WORK STATEMENT

Application Migration:

- a. Recommend Azure Infrastructure as a Service (IaaS) migration planning method of initial grouping of workloads based upon their cloud fit rating and input from DC3 Application owners and other DC3 departments.
- b. Conduct detailed assessment and planning with input from application owners to identify workload specific migration steps to be included (e.g., DNS changes, application IP addressing, and firewall/routing changes).
- c. Recommend and conduct Proof-of-Concept testing with one of DC3 application prior to full migration of DC3 application to prove that Azure IaaS can host DC3 application while meeting all DoD/AF requirements.
- d. Develop holistic migration planning includes a process where dependencies are uncovered that may impact the planned migration workload. These dependencies include, but are not limited to:
 1. Compliance (DoD Cloud SRG and Security Technical Implementation Guides (STIGs), etc.) - (IL5).
 2. CS requirement based on DoD RMF.
 3. DoD and Non-DoD user access.
 4. Dependencies to other solutions / integrations Performance.
 5. Connectivity as required by Solution/workload (NIPRNET/INTERNET).
- e. Address assessment and implementation of development operations (DevOps) and Azure data platform as separate workloads.
- f. Allow DC3 access during the application migration, to a single-pane-of-glass to launch assessments, analyze workload dependencies, properly size assets, view financial projects and comparisons, and understand the dependencies for application migration to ensure a successful cloud adoption and to help the Government make decisions, both business and technical.

C.5.8.11 SUBTASK 8.11 – STRATEGIC PLANNING AND POLICY

The contractor shall provide policy and planning expertise to perform DC3 strategic planning, cyberspace operations planning, exercise planning, and analysis for complex cyber programs. The support requires extensive operational coordination with other National, DoD, and AF programs. Programs relate to one or more of the following strategic or operational areas: cyber training (DC3/CTA), cyber forensic and analytical capability development, D/MM forensic examinations, cyber investigations and operations, cyber threat analysis and DIB information sharing, cyber operations data management and sharing, and the critical infrastructure protection specifically focused on the DIB.

The contractor shall support continual assessment, interpretation, and implementation of National, DoD, and AF strategies and guidance for application to DC3 missions through development of organizational and resourcing strategies, implementing policies, and annual performance measurements. The contractor shall consult and coordinate with staff from other DoD organizations and Federal agencies to interpret, develop, and modify strategies and policies to ensure efforts meet program needs. The contractor shall keep abreast of changes in policy direction and assess impacts on DC3 mission requirements. The contractor shall present findings

Task Order 47QFCA22F0025

Modification P00001

PAGE C-44

SECTION C – PERFORMANCE WORK STATEMENT

to DC3 leadership and make recommendations for improvement where appropriate. The contractor shall assist DC3 with the development and sustainment of the organizational Strategic Plan and implementing policy documents; development and sustainment of the DC3 performance measurement program; as well as the development, implementation, and management of process improvement plans.

The contractor shall support DC3 in cyber exercise planning, execution, participation, evaluation, and reporting. As a Federal Cybersecurity Center, DC3 participates in several national, intelligence community, and DoD cyber exercises to objectively evaluate DC3's role to share cyber threat information, contribute to national response of cyber incidents of significant consequences, and exercise our ability to integrate with the response community. The contractor shall assist DC3 leadership with developing exercise goals, objectives, scenarios, and injects. Upon cyber exercise commencement, the contractor shall assist in the development of lessons learned and after-action items and contribute to exercise after action reports as applicable.

The contractor shall coordinate on and prepare responses to mission-related administrative taskings from the DC3 Civilian Leader (CL) and higher echelons. This includes staffing taskings with appropriate DC3 Directorates; evaluating, deconflicting, and aggregating inputs received; analyzing facts; performing appropriate research; and applying functional expertise to prepare recommended responses for DC3 leadership (e.g., DC3 coordinated and prepared responses to over 400 mission-related administrative taskings in Calendar Year (CY) 2019). The contractor shall provide timely and accurate development of staff packages, staff studies, and papers IAW AF Handbook 33-337, The Tongue and Quill and AFMAN 33-326, Preparing Official Communications.

The contractor shall support the tracking and coordination of agreements between DC3 and DC3's external customers for the Government's review and approval. In CY 2020, DC3 executed 78 separate agreements. The types of agreements include, but are not limited to: Memorandum of Agreement, Memorandum of Understanding, Support Agreements (DD Form 1144 and/or FS Form 7600), and technology transfer mechanisms that include Cooperative Research and Development Agreements, Educational Partnership Agreements, Articulation Agreements with educational institutions, Software Licensing Agreements and other technology transfer mechanisms as authorized by United States Airforce (USAF) and DoD in DC3's roles and responsibilities as a DoD laboratory and technical activity and Office of Research and Technology Applications. Efforts entail clarifying and documenting requirements and expectations of all parties to the agreement and ensuring resource implications are properly addressed. The contractor shall support timely development of Agreements IAW DoDI 4000.19 and AF Instruction (AFI) 25-201, and DC3 Instruction 25-1; and the timely development of technology transfer mechanisms IAW DoDD 5535.03, DoDI 5535.08, AFI 61-301 and the AF Technology Transfer Handbook. DC3 currently manages 122 active agreements with external parties. The contractor shall support the DC3 Support Agreement Manager and Functional Area Agreement Coordinator and provide non-inherently Governmental assistance in reviewing, revising, renewing and/or terminating all agreements on an annual basis.

C.5.8.12 SUBTASK 8.12 – MISSION PARTNER LIAISON SUPPORT

The contractor shall support efforts as a liaison with other DoD organizations and Federal agencies to integrate DC3 policy, planning, and resource actions as a Federal Cybersecurity

Task Order 47QFCA22F0025

Modification P00001

PAGE C-45

SECTION C – PERFORMANCE WORK STATEMENT

Center. This includes promoting the exchange of information on requirements, capabilities, deficiencies, as well as emerging technologies and cyber threats.

The contractor shall assist DC3 leadership with presenting, justifying, and defending DC3 positions and work collaboratively with DC3's external mission partners to achieve common understanding and reasonable resolution of controversial issues related to DC3's mission. The contractor shall coordinate efforts to minimize operational conflicts and/or duplication in order to best achieve overall DoD and National strategies related to core DC3 cyber missions.

In support of these efforts, DC3 regularly hosts and attends planning meetings with external mission partners to include Federal Cybersecurity Centers, Law Enforcement (LE), USIC and DoD. The meeting topics cover a broad scope of mission-related activities including training, Forensic Examinations, Forensic Tool Development, LE/CI Threat Analysis, and DIB CS support. On average, the in-person meetings are held approximately once a week at a minimum. As such, the contractor shall facilitate and/or attend meetings, forums, working group sessions, and conferences; develop and present informational briefings; develop and/or analyze read-ahead material; provide historical records; and document and analyze results from such sessions.

C.5.8.13 SUBTASK 8.13 – INFORMATION MANAGEMENT (IM), KNOWLEDGE MANAGEMENT (KM), RECORDS MANAGEMENT (RM), AND PUBLICATIONS AND FORMS MANAGEMENT

The contractor shall assist in developing, implementing, and maintaining an information, knowledge, and records management capability. This capability shall address enterprise-wide DC3 electronic and records management systems (including knowledge management and information management systems) and establish standardized Information Management (IM)/Knowledge Management (KM)/Records Management (RM) practices, ontologies, taxonomies, meta-data tagging schemas, and management controls in support of DC3 document and record systems, including classification, retrieval and retention processes. The IM/KM/RM capability shall address acquisition of information from one or more sources, the custodianship and the distribution of that information, and disposition of it through archiving or deletion. The IM/KM/RM capability must address the accounting and administration of digital content throughout its lifecycle, from creation to permanent storage or deletion. The digital content will consist of images, video, audio, and multimedia, as well as text. The contractor shall develop and document IM/KM/RM standards, ontology, and taxonomies for lifecycle management and records management of information and data acquired, processed, used, stored, and disposed by the DC3.

The contractor shall document and maintain the IM/KM/RM SOPs (**Section F, Deliverable 37**). The contractor shall assist in the development, coordination, approval, and publishing of DC3 publications and forms, and ensure accessibility to DC3 users. This includes ensuring the annual review and/or periodic validation of the DC3 inventory of publications and forms. The contractor shall assist the IM/KM/RM in documenting strategic, operational, and tactical processes into SOPs for operational efficiency and continuity of operations requirements (**Section F, Deliverable 37**).

SECTION C – PERFORMANCE WORK STATEMENT

C.5.8.14 SUBTASK 8.14 – DC3 FACILITIES AND LOGISTICS MANAGEMENT

The Government is implementing lifecycle accounting of its key assets to include IT equipment, peripherals, and software that include those developed by its TSD Directorate. While many of these items will be accounted by the DPAS system, it is imperative that the contractor shall ensure all logistics actions and procurements are recorded and reported monthly, appropriate metrics are maintained in format requested, and that these metrics are made available to the Government for review and approval. The contractor shall support DC3 contracting procurement requirements by researching alternatives to asset requisitioning; timely input of requisitions IAW supporting contracting office and the Federal Acquisition Regulation (FAR); coordination with supporting Government Purchase Card (GPC) program and large purchase contract offices; and tracking orders to receipt, formal issue of items to end user, full accountability of assets in use, and proper disposal of assets at lifecycle end. The contractor shall work with the Government to develop processes that support contractor and Government operations for the logistics operations.

The contractor shall provide standard supply chain management support to inventory control and accountability, and vehicle management functions for DC3 review and approval. This shall include implementing and sustaining DC3's material and equipment inventories, asset receipt and disposal, routine and large purchasing actions for DC3's IT assets and the agency's related mission, vehicle fleet management system support, mail room services management support, IT software and hardware, and other logistics functions. However, the contractor shall not determine what Government property is to be disposed of and on what terms. The contractor shall have cross-trained contractor staff to avoid single points of failure.

DC3 currently utilizes a self-service SharePoint capability for vehicle fleet management. The Government intends to move this capability into Jira or equivalent automation tool in order to centralize the management and metrics of vehicle use. The capability will continue to support self-service as well as tracking of administrative functions, such as vehicle checks, fluid level checks, and condition reporting, and form automation capabilities. The contractor shall use software as provided by the Government. The Government uses the Defense Property Accountability System (DPAS) for procurement, transportation, inventory, and logistics requests.

The contractor shall support DC3's facilities and infrastructure program IAW AF and DoD policies and regulations. The contractor support shall include but is not limited to maintaining and generating reports and metrics, tracking of facilities projects, and other facilities management and infrastructure activities.

The contractor shall maintain a DC3 space program which includes seat allocation in software platform provided, space plan development, use of software such as AutoCAD or Visio to develop space layouts, and future space usage plans. The contractor shall assist in development of processes that provide integrated contractor and Government facility operations.

The contractor shall review and respond to DC3's facilities and logistics service desk tickets. The contractor shall provide responsive and timely resolution for facilities and logistics-related issues. The contractor shall ensure all facilities issues and incidents are recorded and reported monthly, appropriate metrics are maintained, and that these metrics are made available to the Government.

Task Order 47QFCA22F0025
Modification P00001

PAGE C-47

SECTION C – PERFORMANCE WORK STATEMENT

The contractor shall have the personnel to support facilities and logistics emergencies in coordination with the Government within one hour by phone and within two hours in person.

The contractor shall perform all support IAW DoD guidance, AF policies, DC3 instructions, and guidance.

The contractor shall assist the LG/FAC in documenting strategic, operational, and tactical processes into SOPs for operational efficiency and continuity of operations requirements (Section F, Deliverable 38).

C.5.8.15 SUBTASK 8.15 – HUMAN RESOURCES (HR) MANAGEMENT AND WORKFORCE DEVELOPMENT

The contractor shall assist DC3's HR management system with personnel, manpower, and administrative functions such as maintaining and generating reports and metrics and other HR management activities relating to the Unit Manpower Document and associated duties. However, the contractor shall not participate in: 1) the selection or non-selection of individuals for DC3 employment, including the interviewing of individuals for employment; and 2) the approval of position descriptions and performance standards for DC3 employees.

The contractor shall stay abreast of the latest AF and DoD guidance and policies and perform work IAW the latest policies and procedures.

The contractor shall track the execution of DC3 personnel actions, provide analysis of HR guidance, and provide full spectrum reporting of DC3's HR program management.

The contractor shall provide subject matter expertise to assist HR with both workforce and workload analysis capabilities so as to modernize its workforce and its human capital capabilities. The role of HR is vital to an organization, particularly workload analysis. The contractor shall provide subject matter expertise to assist HR with reviewing the current state of human resources, categorizing jobs, defining the scope of analysis, measuring the ideal number of employees needed, and determining the adequate solution.

The contractor shall develop an internal manpower database consisting of all personnel authorized and assigned to DC3 to include government, military, and contractor personnel. This database shall coordinate with those used by Facilities (location/seating charts) and Security (clearance/badge issuances) to ensure full accountability of all personnel assigned to DC3. The contractor shall coordinate with the Directorates to automate and provide a weekly personnel and manpower status report and update the manpower database upon notification of incoming and outgoing personnel actions. The contractor shall assist HR with the DC3 in and out-processing system to include coordinating with ER for contractors and AF Superintendent for military assignments. The contractor shall also update and enhance BTO business metrics with the most current personnel and manpower data and provide Financial Management manpower statistics in response to higher headquarters tasking.

The contractor shall assist with the periodic validation of Mission Essential, Information Assurance and Cyber Workforce position codes and other related reports to ensure updates are submitted and updated correctly into Defense Civilian Personnel Data System (DCPDS).

The contractor shall assist in developing and implementing a talent management and workforce development plan and program and provide recommendations for improving the current

Task Order 47QFCA22F0025

Modification P00001

PAGE C-48

SECTION C – PERFORMANCE WORK STATEMENT

workforce and assuring DC3 maintains a competitive, well-trained, robust talent pool. These duties shall include activities such as:

- a. Providing recommendations on the organizational structure strategies to include job series, grade, duty title, and supervisory level that creates a developmental path for the workforce.
- b. Creating electronic templates and guidelines for developing consistent and standardized position descriptions that support approved organizational structures.

The contractor shall provide technical assistance with the annual nomination call to assist Directorates in requesting positions for interns to include measures for maintaining oversight of receipt of internship billets and coordinate with applicable Directorate and hiring manager to prepare required hiring documentation from the creation of a position description, training plan, interview process, and onboarding and ensure all information can be tracked and verified upon request.

The contractor shall develop, implement, and maintain a DC3-wide training management program that can be used to centrally manage all training requirements on behalf of DC3 personnel. The program shall be a support mechanism for acquiring, coordinating, and tracking DC3 training requirements as well as maintaining compliance with DoD/USAF personnel certifications and training. The training requirements primarily consist of external (third-party vendor) training and distance learning requirements.

The contractor shall assist HR in accounting and electronically tracking all DC3 assigned personnel to ensure they possess the appropriate DoD 8570 and cyber workforce certifications for those assigned to positions requiring Information Assurance Technician (IAT) Level I, II, or III; Cloud Environment; Software Developer; or Secure Coding. The contractor shall assist in informing personnel whose certifications require updates or additional education credits to maintain currency.

The contractor shall review and respond to DC3's HR service desk tickets. The contractor shall provide responsive and timely resolution for HR Management, Workforce Development, and Training-related issues.

The contractor shall assist HR in documenting strategic, operational, and tactical human resource and workforce management processes into SOPs for operational efficiency and continuity of operations requirements (**Section F, Deliverable 39**).

C.5.8.16 SUBTASK 8.16 – DC3 PUBLIC AFFAIRS OFFICE (PAO) SUPPORT

The contractor shall support strategic, operational, and tactical communication efforts to enhance DC3's internal and external messaging and outreach, including audience surveys, analysis, and targeting. The support includes summarizing highly complex technical issues into consumable information via a variety of ad-hoc projects in digital communications, marketing, graphics, and general outreach support for the DC3 organization.

The contractor shall assist in establishing communications standards and electronic methods for various communications channels, such as DC3 periodicals web services, publications, presentations, etc. The contractor shall establish a consistency for branding, customer

SECTION C – PERFORMANCE WORK STATEMENT

engagement, and reduction of duplication or disparate information management artifacts. The contractor shall support news and informational emails sent to internal and external recipients.

The contractor shall provide an electronic method to create, distribute, and store DC3 physical and virtual media artifacts. The contractor shall update and maintain the operating instructions for all outreach communications activities.

The contractor shall, with Government review and approval, assist in coordinating all press and media activity-related requests at DC3, all visitors and tours of DC3, and all DC3 briefings and speaker engagements.

The contractor shall provide digital photography and graphics support for the planning and designing of concepts to represent internal and external communications initiatives. This includes but is not limited to: Multimedia Production (animations), Physical Media Production (compact discs (CDs)/digital video discs (DVDs)), DC3 logos, artwork, flyers, brochures, templates and layout for websites, email marketing blasts, newsletters, white papers, brochures, articles, and other written documents.

The contractor shall review and respond to DC3's PAO service desk tickets. The contractor shall provide responsive and timely resolution for PAO-related issues.

The contractor shall establish a strategic engagement program that maps to DC3 stakeholders, mission partners, and counterparts; mapping to recurring engagements driving to a clear ends, messaging, and priorities; and assist DC3 in executing approach to scheduling, tracking, and managing the strategic engagement program.

The contractor shall assist the PAO in documenting strategic, operational, and tactical engagements and communications into SOPs for operational efficiency and continuity of operations requirements (**Section F, Deliverable 40**).

C.5.8.17 SUBTASK 8.17 – DC3 SECURITY MANAGEMENT

Security management is the identification of an organization's assets (including people, buildings, machines, systems and information assets), followed by the development, documentation, and implementation of policies and procedures for protecting assets. The contractor shall provide assistance in coordinating with Chief Information Security Officer (CISO) as necessary to ensure smooth continuity of security objectives.

The contractor shall assist the Government in supporting the continuous maintenance of DC3's physical, information, and personnel security program IAW AF and DoD policies and instructions. DC3 currently uses e-QIP, Scattered Castles, and the Defense Information Security System (DISS) for personnel security processing. Security personnel supporting this contract are required to possess a Top Secret (TS) Sensitive Compartmented Information (SCI) clearance in order to obtain a JWICS account for communicating on sensitive security matters (e.g., Sensitive Compartmented Information Facility (SCIF) accreditation/re-accreditation packages).

The contractor shall work with DC3's security office to ensure the security of DC3 IT assets, ensure classified information is handled and discarded IAW DoD policy, manage DC3's SCIFs, manage personnel clearances, maintain access controls to DC3 IT assets, and other security related functions.

SECTION C – PERFORMANCE WORK STATEMENT

The contractor shall provide support for the electronic facility alarm systems, Closed Circuit Television (CCTV) controls, access control methods and emergency response procedures, and conduct security surveys and assessments.

C.5.9 TASK 9 – JUDGE ADVOCATE (JA) OFFICE SUPPORT

The contractor shall provide IT and Cyber Forensics paralegal expertise to the JA Office. These services shall consist of drafting, revising, and organizing via electronic means legal opinions, litigation support and recommended training pertinent to ongoing cyber investigations/trials being conducted by DC3. The contractor shall provide electronic work management solutions within the JA office that includes the ability to organize meetings, track communications, obtain resources and logistics support, track the workflow of assigned items. The contractor shall not engage in any personal services or inherently Governmental functions to the JA Office.

The contractor shall provide technical assistance to the JA Office regarding the office's review and response to requests made under the Freedom of Information Act (FOIA), the Privacy Act, Congressional inquiries, and Ethics, Intelligence Oversight, Uniform Code of Military Justice (UCMJ) Article 6, Inspector General, or other inquiries and inspections for Government review and approval only as it pertains to the IT expertise that DC3 needs to conduct these inquiries.

The contractor shall make recommendations that compare gathered information/electronic evidence against the Fourth Amendment and Electronic Communication Privacy Act in regard to evidence admissibility (including privilege) standards when making recommendations for the office's disposition concerning forensic information and examinations.

The contractor shall provide assistance to the JA Office with the office's preparation of DC3/CFL examiners for testimony in a court of law, including developing charts and illustrations as trial exhibits to support the examiner in testimony.

The contractor shall obtain and maintain records via electronic methods related to examiner participation as expert witnesses, including soliciting, distributing for review, and maintaining transcripts of testimony and feedback from litigating attorneys.

The contractor shall implement, organize, manage, and maintain, at the Directorate (non-developer) level, the JA Legal Portal and JA ticketing system both as to organization and content pursuant to Attorney Advisor guidance and keep the Attorney Advisor apprised of significant issues regarding operability/utility.

The contractor shall solicit and analyze JA customer feedback pursuant to Attorney Advisor guidance.

C.5.10 TASK 10 – DC3 SURGE SUPPORT

DC3's mission is subject to constant technological and operational change. As such, the contractor shall support the objective of keeping DC3's technological and mission capabilities congruent with developments and changes in the fields of D/MM forensics, CS, and IT through a

SECTION C – PERFORMANCE WORK STATEMENT

surge capability. The contractor shall support the objective of keeping DC3's BTO and ER mission capabilities congruent with developments and changes through a surge capability.

The surge capability shall provide staff resources for unplanned projects or unexpected events (on-call 24x7 support) in the task areas identified throughout Task 2, Task 3, Task 4, Task 5, Task 6 and Task 8 of the PWS; for example, time-sensitive lab cases, running short-term pilot programs, DIB security-sensitive requests, new technology implementation, system modernization, forensic lab upgrades, policy impacts, and national security/critical events. Project-based surge efforts are anticipated to last six months to a year.

In support of project-based surge efforts, the contractor shall develop a comprehensive Surge Project Plan, inclusive of project scope, requirements, milestones, deliverables, and resource/cost information (**Section F, Deliverable 41**) to be approved by the Government prior to project start, IAW Section H.13 Work Request. The contractor shall staff surge resources within 30 days of formal written approval of the Surge Support Plan.

C.5.11 TASK 11 - EXTERNAL CUSTOMER SUPPORT

The contractor shall provide severable or non-severable services, using any task areas identified throughout Task 2, Task 3, Task 4, Task 5, and Task 6 of the PWS in support of DC3's external customers. Sample severable and non-severable task descriptions are provided in **Section J, Attachment Z**. In support of project-based efforts, the contractor shall develop a comprehensive External Customer Support Project Plan, inclusive of project scope, requirements, milestones, deliverables, and resource/cost information (**Section F, Deliverable 42**) to be approved by the Government prior to project start, IAW Section H.13 Work Request. The contractor shall staff resources within 30 days of formal written approval of the External Customer Support Plan.